English abstract of document FR-A-2 788 867

The cryptographic processing involves product-sum calculations on long numbers, and is implemented as a unitary operation with carry propagation for computation with integer arithmetic, and without carry propagation for computation based on a finite Galois field. Separate integer (11) and Galois field (12) computation circuits are provided, with a selector (13) to choose the appropriate circuit.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 788 867**

(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 00680**

(51) Int Cl[7] : **G 06 F 12/14**, G 06 F 7/12

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 20.01.00.

(30) **Priorité :** 20.01.99 JP 01198999; 23.07.99 JP 20983199.

(43) **Date de mise à la disposition du public de la demande :** 28.07.00 Bulletin 00/30.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *KABUSHIKI KAISHA TOSHIBA* — JP.

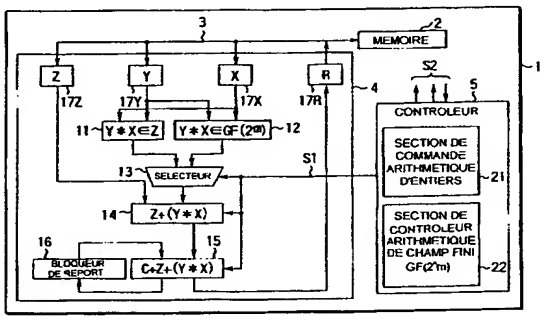
(72) **Inventeur(s) :** SHIBA MASUE et KAWAMURA SCHINICHI.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

(54) PROCEDE ARITHMETIQUE, APPAREIL ARITHMETIQUE ET APPAREIL DE TRAITEMENT CRYPTOGRAPHIQUE.

(57) Un appareil arithmétique pour réaliser une opération produit-somme sur des nombres longs inclut un circuit arithmétique unitaire d'entiers (11), un circuit arithmétique unitaire basé sur champ fini GF (2^m) (12) adjacent du point de vue logique au circuit arithmétique unitaire d'entiers, un sélecteur (13) pour sélectionner soit le circuit arithmétique d'entiers, soit le circuit arithmétique unitaire basé sur champ fini GF (2^m) et un circuit d'additionneur (14) qui comporte un tampon pour stocker des données de résultat intermédiaire, qui additionne les données de résultat intermédiaire aux données de résultat obtenues par soit le circuit arithmétique unitaire d'entiers, soit le circuit arithmétique unitaire basé sur champ fini GF (2^m) selon celui qui est sélectionné par le sélecteur, qui propage un report lors d'une opération arithmétique unitaire basée sur des entiers et qui ne propage pas de report lors d'une opération arithmétique unitaire basé sur champ fini GF (2^m).



FR 2 788 867 - A1

ARRIÈRE-PLAN DE L'INVENTION

La présente invention concerne un procédé arithmétique et un appareil arithmétique ainsi qu'un appareil de traitement cryptographique et plus particulièrement, un procédé arithmétique et un appareil arithmétique ainsi qu'un appareil de traitement cryptographique qui sont utilisés de façon appropriée pour des coprocesseurs cryptographiques et similaire mis en œuvre dans par exemple des cartes à circuit intégré (IC) et des appareils électriques domestiques à flux d'information.

Lors de la mise en œuvre d'un circuit intégré à grande échelle d'intégration (LSI) pour une cryptographie par clé publique, un système cryptographique pour réaliser une opération basée sur les entiers du système RSA (Rivest-Shamir-Adleman) ou similaire a été essentiellement utilisé.

Dans ce système, une opération doit être réalisée pour un entier à l'aide d'un nombre important de chiffres. Pour cette raison, si ce système est appliqué à une carte IC ou similaire, un processeur à usage spécial est requis. Bon nombre de systèmes qui mettent en œuvre de tels coprocesseurs à usage spécial pour réaliser des opérations basées sur des entiers longs pour un traitement cryptographique ont déjà été mis en utilisation pratique.

Récemment, l'attention a été attirée par des systèmes cryptographiques basés sur un système algébrique appelé champ fini GF (2^m) : champ de Galois, tout particulièrement des systèmes cryptographiques à courbe elliptique d'un champ fini GF (2^m), au lieu de systèmes cryptographiques basés sur des entiers.

Dans ce système cryptographique qui utilise une opération arithmétique à champ fini GF (2^m), le nombre de bits à manipuler doit être établi de manière à être aussi important que 160 ou plus comme dans un système à opération basée sur des entiers tel que RSA. Pour cette raison, si un tel système est mis en œuvre sur un dispositif dans lequel la performance d'une unité centrale de traitement ou CPU est

faible, par exemple une carte IC, un temps de traitement relativement long est requis. Par conséquent, il y a des demandes pour une augmentation de la performance en utilisant des composants matériels à usage spécial (des coprocesseurs).

Comme décrit ci-avant, conformément au système RSA ainsi qu'à la cryptographie à courbe elliptique, les coprocesseurs à usage général doivent être préparés afin de réaliser un traitement cryptographique haute vitesse dans des cartes IC et similaire.

La figure 23 représente l'implantation d'un LSI de carte IC incluant un coprocesseur pour un traitement cryptographique. Par report à la figure 23, dans ce LSI, une unité centrale de traitement ou CPU, une mémoire vive ou RAM, une mémoire morte ou ROM et une mémoire morte programme et effaçable électriquement ou EEPROM sont intégrées selon une seule puce et le coprocesseur est constitué par une RAM, par une section arithmétique et par une section de commande. Le coprocesseur assiste la CPU dans la réalisation d'opérations arithmétiques de base pour une cryptographie par clé publique, par exemple une exponentiation sur des nombres longs et les quatre opérations fondamentale de l'arithmétique sous la commande de la CPU.

La figure 24 représente un coprocesseur dans le LSI représenté sur la figure 23. Selon le système RSA, ce composant est mis en œuvre en tant que multiplicateur basé sur les entiers permettant de réaliser des opérations basées sur les entiers.

Lors de l'assemblage d'un LSI d'une cryptographie à courbe elliptique, bien que l'agencement global devienne identique ou similaire à celui du LSI représenté sur la figure 23, un coprocesseur pour réaliser des opérations arithmétiques de champ fini GF (2^m) doit être préparé en lieu et place d'un coprocesseur pour réaliser des opérations basées sur les entiers.

La figure 25 est un schéma fonctionnel qui représente l'agencement de composants matériels d'un coprocesseur pour réaliser

des opérations arithmétiques de champ fini GF (2^m) avec une base de polynôme.

La figure 25 représente un type d'appareil arithmétique pour un champ fini GF (2^m) appelé champ cyclotomique qui utilise le polynôme irréductible spécial décrit dans "Hardware Implementation of Elliptic Curve Cryptosystem", SCIS' 98-10. I.C. Cet appareil arithmétique comporte un agencement permettant d'exécuter des opérations d'addition, d'élévation au carré, de multiplication et d'inversion sur un champ fini GF (2^m). Moyennant cet agencement, une opération arithmétique de champ fini GF (2^m) requise pour calculer un point sur une courbe elliptique est exécutée. En intégrant un tel appareil arithmétique dans un IC, un coprocesseur pour des opérations arithmétiques de champ fini GF (2^m) qui peut être appliqué au LSI de la figure 23 peut être obtenu.

Dans ce cas, chacun des circuits d'additionneur et de multiplicateur est constitué par m portes OU-exclusif, et un circuit de multiplicateur 81 est mis en œuvre au moyen de l'agencement de circuit représenté sur la figure 26.

La figure 26 représente un circuit de multiplicateur basé sur champ fini GF (2^m) appelé champ cyclotomique.

Le circuit de multiplicateur 81 comporte des registres d'entrée de m bits A et B. Le circuit de multiplicateur 81 entre les coefficients d'un polynôme a(x) en tant que valeurs fixes sur le registre d'entrée A et réalise un calcul tout en décalant les coefficients d'un polynôme b(x) à partir du bit de poids le plus fort en réponse à des horloges respectives. Par report à la figure 26, des symboles de référence D représentent des bascules bistables constituant un registre de retour. Lorsque m décalages sont réalisés, les valeurs des blocs respectifs D sont chargées dans un registre de sortie C, d'où ainsi l'obtention de a(x) * b(x) en tant que résultat d'opération.

Comme il apparaît au vu de la comparaison entre les circuits représentés sur les figures 24 et 26, une opération de multiplication basée sur les entiers et une opération arithmétique de champ fini GF

(2^m) d'une base polynôme diffèrent totalement du point de vue de leur architecture pour exécuter des opérations de multiplication. Des tentatives ont par conséquent été faites afin de former des agencements de composants matériels différents pour les systèmes cryptographiques respectifs.

Pour une multiplication modulaire basée sur champ fini GF (2^m) lors d'une opération fondamentale pour un système cryptographique à courbe elliptique, un appareil arithmétique qui utilise un registre décalage à retour linéaire (LFSR) en tant que circuit de division qui utilise un polynôme f(x) sur un champ fini GF (q^m) est largement utilisé. Le polynôme modulo f(x) est :

$f(x) = f_m x^m + f_{m-1} x^{m-1} + \ldots + f_1 x + f_0$ . . $f_m = 1$

La figure 27 est un schéma fonctionnel qui représente l'agencement d'un registre à décalage à retour linéaire LFSR. Dans ce LFSR 90, des additionneurs OU-exclusif 91_1 à 91_m et des éléments de retard d'une horloge (appelés ci-après des registres) 92_1 à 92_m sont montés en cascade en alternance depuis le côté d'entrée. Dans cet agencement, la sortie qui est extraite depuis le m-ième registre à décalage 92_m est appliquée en retour séparément sur les m additionneurs 91_1 à 91_m par l'intermédiaire d'unités de coefficient 93_1 à 93_m.

Ce LFSR 90 fonctionne sur une base temps unitaire (horloge). Dans le registre à décalage, l'avancement d'une impulsion d'horloge opératoire d'une horloge est appelé réalisation d'un décalage et le nombre m de registres 92_1 à 92_m incorporés dans le registre à décalage est appelé nombre d'étages du registre à décalage.

Lorsque q = 2, une bascule bistable d'un bit peut être appliquée à chacun des registres 92_1 à 92_m. Chacune des unités de coefficient 93_1 à 93_m multiplie "1" ou "0". Lorsque "1" est multiplié, une unité de coefficient correspondante est connectée tandis que lorsque "0" est multiplié, une unité de coefficient correspondante n'est pas connectée. En tant que chacun des additionneurs 91_1 à 91_m, une porte OU-exclusif à deux entrées est utilisée.

Dans ce LFSR 90, lorsque les coefficients d'un polynôme de dividende sont entrés séquentiellement depuis le côté d'entrée (le côté gauche) en partant des ordres plus élevés, les coefficients d'un polynôme de quotient sont émis en sortie de façon séquentielle depuis le côté de sortie (le côté droit) en partant des ordres plus élevés. Dans ce cas, les contenus des registres respectifs (les bascules bistables) 92_1 à 92_m suite à la fin de l'entrée du terme d'ordre 0 du polynôme de dividende sont les coefficients d'un polynôme de reste.

Dans l'appareil arithmétique qui utilise le LFSR 90 mentionné ci-avant, cependant, les registres 92_1 à 92_m dont le nombre est égal au nombre de bits d'un degré m sont requis et il s'ensuit que l'agencement des registres 92_1 à 92_m est limité par le degré m. Par conséquent, si le degré m augmente, le LFSR doit être modifié pour chaque appareil arithmétique. Bien que l'invention soit présentement dédiée à des systèmes cryptographiques à courbe elliptique, des systèmes cryptographiques RSA sont encore dans le cadre de l'invention. Il est par conséquent fortement requis que même des cartes IC qui utilisent des systèmes cryptographiques à courbe elliptique puissent être adaptées avec des systèmes cryptographiques RAS.

Lorsqu'à la fois un système cryptographique basé sur des entiers classique et un système cryptographique basé sur champ fini GF (2^m) doivent être incorporés dans la même carte IC, des coprocesseurs correspondant aux systèmes cryptographiques respectifs doivent être incorporés dans la carte IC selon les techniques classiques. Cependant, si deux coprocesseurs sont incorporés dans la carte IC, l'aire de puce de la carte IC qui est fortement limitée en termes d'aire est réduite de façon non souhaitable.

Lors d'une multiplication modulaire basée sur champ fini GF (2^m), lorsque le degré m augmente, le LFSR doit être modifié pour chaque appareil arithmétique, ce qui impose des limitations en termes de composants matériels.

RÉSUMÉ DE L'INVENTION

Un objet de la présente invention consiste à proposer un procédé arithmétique et un appareil arithmétique ainsi qu'un appareil de traitement cryptographique qui puissent exécuter des opérations arithmétiques sans modifier les configurations d'appareil même si le degré m d'un champ fini GF (2^m) augmente.

Un autre objet de la présente invention consiste à proposer un appareil arithmétique et un appareil de traitement cryptographique qui puissent exécuter une opération arithmétique de champ fini GF (2^m) ainsi qu'une opération basée sur des entiers en additionnant seulement des architectures minimum.

Selon la présente invention, on propose un appareil arithmétique qui fonctionne en tant que circuit arithmétique unitaire tout en propageant un report lors d'une opération arithmétique unitaire basée sur des entiers et tout en faisant fonctionner le circuit arithmétique unitaire sans propager un quelconque report lors d'une opération arithmétique unitaire basée sur champ fini GF (2^m).

Selon la présente invention, une opération arithmétique de champ fini GF (2^m) peut être exécutée de même qu'une opération basée sur des entiers en additionnant seulement une architecture minimum.

Selon la présente invention, on propose un appareil arithmétique comprenant un circuit arithmétique unitaire basé sur des entiers, un circuit arithmétique unitaire basé sur champ fini GF (2^m) qui est adjacent du point de vue logique au circuit arithmétique unitaire basé sur des entiers et un sélecteur pour sélectionner le circuit arithmétique unitaire basé sur des entiers ou le circuit arithmétique unitaire basé sur champ fini GF (2^m).

Selon la présente invention, une opération de multiplication unitaire basée sur des entiers et une opération de multiplication basée sur champ fini GF (2^m) peuvent toutes deux être exécutées en additionnant seulement un circuit arithmétique unitaire basé sur champ fini GF (2^m).

Selon la présente invention, l'appareil arithmétique comprend un circuit arithmétique unitaire basé sur les entiers et un circuit de commande de sélection qui émet en sortie sur le circuit arithmétique unitaire basé sur les entiers un signal de sélection pour sélectionner une opération arithmétique unitaire basée sur les entiers ou une opération arithmétique unitaire basée sur champ fini GF (2^m). En outre, le circuit arithmétique unitaire basé sur les entiers comprend un circuit de commande de propagation de report qui, lors de l'exécution d'une opération de produit-somme sur des nombres longs, propage un report suite à la réception d'un signal de sélection qui demande en instruction une opération arithmétique unitaire basée sur les entiers, et qui ne propage pas de report suite à la réception d'un signal de sélection qui demande en instruction une opération arithmétique unitaire basée sur champ fini GF (2^m). Dans cet appareil, le mode arithmétique basé sur les entiers et le mode arithmétique basé sur champ fini GF (2^m) peuvent être commutés en commandant une propagation de report dans le circuit arithmétique unitaire.

Selon la présente invention, une opération arithmétique basée sur les entiers et une opération arithmétique basée sur champ fini GF (2^m) peuvent toutes deux être exécutées en additionnant seulement le circuit de commande de propagation de report.

Selon la présente invention, est proposé un appareil arithmétique comprenant un circuit de commande de propagation de report qui réalise une commande de propagation de report dans un additionneur complet selon des unités de bits en utilisant un commutateur sur lequel un signal de sélection et un signal de sortie de report sont entrés.

Dans l'appareil arithmétique de la présente invention, le circuit de commande de propagation de report comprend un sélecteur qui réalise une commutation entre l'émission en sortie d'un résultat OU-exclusif de deux entrées dans un additionneur complet selon des unités de bits en tant que résultat d'addition et l'émission en sortie d'un résultat

OU-exclusif du résultat c et d'un report d'entrée en tant que résultat d'addition.

Selon la présente invention, est proposé un appareil arithmétique comprenant un circuit d'additionneur pour réaliser une addition en propageant un report lors de l'exécution d'une opération de multiplication basée sur les entiers et pour réaliser une addition sans propager un quelconque report lors de l'exécution d'une opération de multiplication basée sur champ fini GF (2^m). Selon la présente invention, une opération de multiplication basée sur les entiers et une opération arithmétique basée sur champ fini GF (2^m) peuvent toutes deux être exécutées de façon fiable en relation avec une partie d'addition d'une opération de produit-somme.

Selon la présente invention, on propose un appareil de traitement cryptographique permettant de réaliser une commutation entre un cryptage ou un décryptage sur la base d'une opération basée sur les entiers qui est réalisée par un appareil arithmétique et un cryptage ou un décryptage sur la base d'une opération arithmétique basée sur champ fini GF (2^m) qui est réalisée par l'appareil arithmétique.

La présente invention peut réaliser à la fois un traitement cryptographique basé sur une opération basée sur les entiers tel qu'une opération cryptographique RSA et un traitement cryptographique basé sur une opération arithmétique basée sur champ fini GF (2^m) tel qu'une opération cryptographique de courbe elliptique.

Selon la présente invention, on propose un appareil arithmétique comprenant une section arithmétique incluant un circuit d'opération de produit-somme sur des nombres longs pouvant exécuter une multiplication modulaire avec une expression basée sur polynôme d'un champ fini GF (2^m) et une section de commande qui commande le circuit d'opération de produit-somme pour exécuter une multiplication modulaire suite à la division de la multiplication modulaire selon un traitement de multiplication et un traitement modulo.

Selon l'appareil arithmétique de la présente invention, puisque le circuit d'opération de produit-somme sur des nombres longs réalise une multiplication modulaire en lieu et place d'un registre à décalage à retour linéaire, un degré arbitraire égal ou supérieur à l'unité peut être utilisé. Par conséquent, même si le degré d'un champ fini GF (2^m) augmente, une opération arithmétique peut être exécutée sans modifier la configuration de l'appareil.

Selon la présente invention, le circuit d'opération de produit-somme comprend un circuit de multiplicateur simple précision configuré pour multiplier des données de polynôme de la base polynôme basée sur champ fini GF (2^m) sans propager un quelconque report et un circuit d'additionneur double précision configuré pour additionner en utilisant un résultat de multiplication obtenu au moyen du circuit de multiplicateur, et l'unité de commande commande le circuit de multiplicateur et le circuit d'additionneur lors du traitement de multiplication.

Selon la présente invention, est proposé un appareil arithmétique comprenant un circuit d'acquisition de quotient qui est commandé par l'unité de commande, pour établir le résultat de multiplication de deux données de polynôme en tant que données de polynôme de premier dividende dans un modulo, pour établir des données de polynôme modulo prédéterminées en tant que données de polynôme de diviseur, pour calculer un quotient sur la base des données de polynôme de premier dividende ou de dividende suivant et des données de polynôme de diviseur et pour acquérir des données de polynôme de quotient d'un bloc, le nombre de bits correspondant à une larguer de bus à partir d'un ordre supérieur. Dans cet appareil arithmétique, l'unité de commande commande le circuit d'acquisition de quotient lors d'une multiplication modulaire et commande le circuit de multiplicateur et le circuit d'additionneur lorsque des données de polynôme de quotient d'un bloc sont acquises. Moyennant cette opération, des données de polynôme de dividende qui suivent sont calculées en soustrayant le résultat de multiplication des données de

polynôme de quotient d'un bloc et des données de polynôme de diviseur à partir des données de polynôme de dividende courantes et le traitement, depuis la commande du circuit d'acquisition de quotient jusqu'au calcul des données de polynôme de dividende, est répété, d'où ainsi l'obtention de données de reste.

Dans cet appareil arithmétique, chaque résultat de multiplication de données de polynôme de quotient d'un bloc et de données de polynôme de diviseur devient (m + 1) blocs.

En outre, ce résultat de multiplication est soustrait du (= est additionné au) polynôme de dividende courant afin de calculer les données de polynôme de dividende qui suivent de (2m - 1*n) blocs (n est le nombre de fois des opérations de multiplication). C'est-à-dire que les données de polynôme de dividende qui précèdent sont diminuées selon des unités de blocs.

A l'aide de l'unité de commande mentionnée ci-avant, la présente invention peut réaliser un calcul de quotient et modulo efficace en utilisant les caractéristiques des composants matériels.

Lors d'un calcul de quotient, le circuit d'acquisition de quotient de l'appareil arithmétique de la présente invention multiplie les données d'inversion des deux blocs supérieurs des données de polynôme de diviseur et les données de polynôme de dividende courantes et établit le second bloc supérieur du résultat de multiplication en tant que données de polynôme de quotient d'un bloc.

A l'aide du circuit d'acquisition de quotient mentionné ci-avant, la présente invention peut extraire une partie de nombre effective à partir du polynôme de quotient obtenu et par conséquent elle peut optimiser la précision opératoire.

Selon la présente invention, est proposé un appareil arithmétique comprenant un circuit d'acquisition de quotient pour calculer des données d'inverse à partir des deux blocs supérieurs des données de polynôme de diviseur et pour stocker les données dans une mémoire lors de l'acquisition de données de polynôme de quotient lors d'une première opération et pour lire les données d'inverse à partir de la

mémoire et pour utiliser celles-ci lors de l'acquisition de données de polynôme de quotient lors d'une seconde opération et des opérations qui suivent.

Selon la présente invention, à l'aide du circuit d'acquisition de quotient mentionné ci-avant, lorsqu'un modulo redondant est exécuté sous le même polynôme modulo, un quotient peut être acquis en lisant des données d'inversion à partir de la mémoire. Par conséquent, le temps requis pour calculer des données d'inversion peut être économisé dans le second calcul de quotient et dans les calculs de quotient qui suivent, et le temps de traitement pour une opération arithmétique de champ fini GF (2^m) peut être raccourci. En outre, puisque les données d'inversion peuvent être calculées à l'avance, une multiplication modulaire basée sur champ fini GF (2^m) peut être réalisée en utilisant seulement le circuit d'opération de produit-somme pour réaliser des opérations de multiplication et d'addition.

Selon la présente invention, est proposé un appareil arithmétique comprenant un circuit d'acquisition de quotient pour, lors du calcul de données d'inverse, compter le nombre de chiffres 0 consécutifs depuis un ordre supérieur de deux blocs supérieurs des données de polynôme de diviseur, extraire des données de polynôme d'un bloc +1 bit à partir de bits d'ordre supérieur de telle sorte que le bit de poids le plus fort soit établi à 1, obtenir l'inverse des données de polynôme extraites, obtenir des données de deux blocs en tant qu'ensemble en concaténant des données corrigées dont le bit de poids le plus faible est de 1 et dont les autres bits sont 0 avec le bit de poids le plus fort de l'inverse obtenu et en établissant en tant que données d'inverse un résultat obtenu en effectuant un décalage binaire des données en direction d'un coté d'ordre supérieur de la valeur de comptage du nombre de 0.

Avec le circuit d'acquisition de quotient mentionné ci-avant, la présente invention utilise une valeur corrigée en tant que données d'inversion afin d'éviter la normalisation d'un diviseur, la correction d'un quotient approché et la dénormalisation d'un résultat d'opération tel

qu'un quotient ou un reste sur la base de l'algorithme de Knuth [références : Knuth, D. E., "The Art of Computer Programming", Vol. 2, Reading, Mass : Addison Wesley, 2nde édition, (1981)] qui utilise une opération de division simple précision utilisée pour une opération de division basée sur les entiers longs générale. Le nombre de fois de décalages de bits peut par conséquent être diminué, et l'appareil arithmétique peut être optimisé.

Selon la présente invention, est proposé un appareil de traitement cryptographique permettant de réaliser un cryptage ou un décryptage sur la base d'une multiplication modulaire basée sur champ fini GF (2^m) au moyen de l'appareil arithmétique.

A l'aide de l'appareil arithmétique, la présente invention peut réaliser un cryptage ou un décryptage sur la base d'une multiplication modulaire basée sur champ fini GF (2^m) telle qu'une opération cryptographique de courbe elliptique.

BRÈVE DESCRIPTION DES DESSINS

La figure 1 est un schéma fonctionnel qui représente un exemple de l'agencement d'un appareil arithmétique selon le premier mode de réalisation de la présente invention ;

les figures 2A, 2B et 2C sont des vues qui représentent un exemple de l'agencement d'un circuit arithmétique unitaire de 4*4 bits qui met en œuvre c'(x) = a(x) * b(x) ;

les figures 3A, 3B, 3C et 3D sont des vues qui représentent un exemple de l'agencement d'un circuit arithmétique unitaire de 4*4 bits qui met en œuvre une opération de multiplication basée sur les entiers ;

la figure 4 est un schéma fonctionnel qui représente un exemple de l'agencement d'un additionneur complet du type report simultané 4 bits muni d'une fonction de commande de report qui est utilisé dans le coprocesseur du premier mode de réalisation ;

la figure 5 est un schéma de circuit qui représente un exemple de l'agencement d'un additionneur complet et d'un commutateur de commande de report qui sont utilisés dans un circuit d'additionneur selon le premier mode de réalisation ;

la figure 6 est un schéma de circuit qui représente une modification de l'additionneur complet muni de la fonction de commande de report ;

la figure 7 est un schéma de circuit qui représente une autre modification de l'additionneur complet muni de la fonction de commande de report ;

la figure 8 est un schéma fonctionnel qui représente un exemple de l'agencement d'un appareil arithmétique selon le second mode de réalisation de la présente invention ;

les figures 9A et 9B sont des vues qui représentent un exemple de l'agencement d'un circuit arithmétique unitaire 4*4 bits qui met en œuvre un circuit de multiplicateur selon le second mode de réalisation ;

la figure 10 est un schéma fonctionnel qui représente un exemple de l'agencement de coprocesseur appliqué à un appareil arithmétique et à un appareil de traitement cryptographique selon le troisième mode de réalisation de la présente invention ;

la figure 11 est une vue schématique qui représente l'agencement d'un circuit d'acquisition de quotient selon le troisième mode de réalisation ;

la figure 12 est une vue schématique permettant d'expliquer la fonction d'une section de calculateur d'inverse selon le troisième mode de réalisation ;

la figure 13 est une vue schématique qui représente l'agencement de la section de calculateur d'inverse selon le troisième mode de réalisation ;

la figure 14 est un organigramme permettant d'expliquer une multiplication modulaire pour une base de polynôme basée sur champ fini GF (2^m) ;

la figure 15 est une vue schématique qui représente un calcul sur papier pour expliquer un modulo selon le troisième mode de réalisation ;

la figure 16 est une vue schématique qui représente le traitement réalisé par une unité arithmétique selon le troisième mode de réalisation ;

la figure 17 est une vue qui représente les nombres requis d'horloges pour des commandes selon le troisième mode de réalisation ;

la figure 18 est une vue qui représente les nombres requis d'horloges pour des opérations GF (2^{160}) opérations selon le troisième mode de réalisation ;

la figure 19 est une vue qui représente les dimensions de circuit de coprocesseurs selon le troisième mode de réalisation ;

la figure 20 est une vue qui représente des dimensions de circuits additionnels selon le troisième mode de réalisation ;

la figure 21 est une vue qui représente les dimensions de circuits de coprocesseurs conçus spécifiquement pour des opérations GF (2^m) à titre de comparaison selon le troisième mode de réalisation ;

la figure 22 est un schéma fonctionnel qui représente un exemple de l'agencement d'un coprocesseur appliqué à un appareil arithmétique et à un appareil de traitement cryptographique selon le quatrième mode de réalisation de la présente invention ;

la figure 23 est un schéma fonctionnel qui représente un LSI de carte IC incluant un coprocesseur de traitement cryptographique ;

la figure 24 est un schéma fonctionnel qui représente un exemple de l'agencement d'une partie de coprocesseur d'un LSI pour réaliser une opération basée sur les entiers ;

la figure 25 est un schéma fonctionnel qui représente un exemple de l'agencement de composants matériels d'un coprocesseur pour réaliser une opération arithmétique de champ fini GF (2^m) d'une base polynôme ;

la figure 26 est un schéma fonctionnel qui représente un circuit de multiplicateur basé sur champ fini GF (2^m) appelé champ cyclotomique ; et

la figure 27 est un schéma fonctionnel qui représente l'agencement d'un registre à décalage à retour linéaire LFSR général ;

DESCRIPTION DÉTAILLÉE DE L'INVENTION

Chaque mode de réalisation de la présente invention sera décrit ci-après par report aux vues des dessins annexés.

(Premier mode de réalisation)

La figure 1 est un schéma fonctionnel qui représente un exemple de l'agencement d'un appareil arithmétique selon le premier mode de réalisation de la présente invention.

Un appareil arithmétique de ce mode de réalisation qui est formé en tant que coprocesseur 1 est un appareil de multiplicateur de produit-somme de nombres longs permettant de réaliser à la fois une opération de multiplication basée sur les entiers et une opération de multiplication basée sur champ fini GF (2^m). Cet appareil exécute d'autres opérations, telles que des opérations d'addition, d'élévation au carré et d'inversion en commandant ce traitement de multiplication. En incorporant cet appareil arithmétique dans un LSI ou similaire, un appareil de traitement cryptographique permettant de réaliser à la fois un système cryptographique RSA et un système cryptographique à courbe elliptique est formé. Dans ce cas, par exemple, le LSI dans lequel l'appareil arithmétique doit être incorporé est l'appareil représenté sur la figure 23.

Dans ce coprocesseur 1, une unité arithmétique 4 est commandée par une unité de contrôleur 5 afin d'entrer/émettre en sortie des données par l'intermédiaire d'un bus de données de 32 bits 3, sur/depuis une mémoire 2 pour stocker des données au fil d'une opération.

Des données d'entrée en provenance du bus de données 3 sont stockées dans des tampons 17Z, 17Y et 17X et des données de sortie sur le bus de données 3 sont stockées dans un tampon 17R.

Les données d'entrée X et Y sont des données de multiplicande/multiplicateur. Parmi ces données, les données Y sont entrées sur un tampon en tant que données divisées selon des unités

constituées par des chiffres prédéterminés afin d'empêcher qu'une opération de multiplication de beaucoup de chiffres ne soit réalisée en une seule fois. Les données Z sont un résultat intermédiaire qui est produit du fait qu'une opération de multiplication est exécutée selon une pluralité d'étapes. Ces données sont additionnées au produit de XY et un débordement appelé un report C est additionné à la somme, ce qui parachève un cycle. Les données R obtenues en ôtant le report des données résultantes sont émises en sortie sur le bus de données 3 par l'intermédiaire du tampon R en vue d'une utilisation en tant que données Z pour une opération lors du cycle suivant. En répétant ce cycle une pluralité de fois, une opération de multiplication d'entiers longs ou une opération de multiplication basée sur champ fini GF (2^m) ("c'" comme décrit ultérieurement dans un sens strict) est réalisée.

Afin de réaliser l'opération mentionnée ci-avant, en plus des tampons 17X, 17Y, 17Z et 17R, le coprocesseur 1 inclut un circuit de multiplicateur basé sur les entiers 11, un circuit de multiplicateur basé sur champ fini GF (2^m), un sélecteur 13, un circuit d'additionneur 14, un circuit d'additionneur 15, un dispositif de blocage de report 16 et l'unité de contrôleur 5.

Le circuit de multiplicateur basé sur les entiers 11 réalise une opération de multiplication basée sur les entiers pour les données X dans le tampon 17X et pour les données Y dans le tampon 17Y et émet en sortie le résultat sur le sélecteur 13.

Le circuit de multiplicateur basé sur champ fini GF (2^m) 12 exécute une partie (c') d'une opération de multiplication basée sur champ fini GF (2^m) en utilisant les données X dans le tampon 17X et les données Y dans le tampon 17Y et il émet en sortie le résultat sur le sélecteur 13.

Le sélecteur 13 émet en sortie les données qui sont émises en sortie depuis le circuit de multiplicateur basé sur les entiers 11 ou depuis le circuit de multiplicateur basé sur champ fini GF (2^m) 12 sur le circuit d'additionneur 14 conformément à un signal S1 en provenance de l'unité de contrôleur 5.

Le circuit d'additionneur 14 est un additionneur complet qui additionne les données Z dans le tampon 17Z à la sortie de sélecteur et qui émet en sortie la somme sur le circuit d'additionneur 15. Dans ce circuit d'additionneur 14, une addition basée sur les entiers et une addition basée sur champ fini GF (2^m) sont commutées conformément au signal de commande S1. Cette commutation d'addition sera décrite ultérieurement.

Le circuit d'additionneur 15 additionne le report C bloqué dans le dispositif de blocage de report 16 à la sortie en provenance du circuit d'additionneur 14. Le circuit d'additionneur 15 émet ensuite en sortie les 32 bits supérieurs de la somme en tant que report suivant C sur le dispositif de blocage de report 16 et émet également en sortie sur un tampon 17R les 8 bits inférieurs en tant que données R qui sont le résultat d'opération lors de ce cycle. Dans le circuit d'additionneur 15 également, une addition basée sur les entiers et une addition basée sur champ fini GF (2^m) sont commutées conformément au signal de commande S1.

Le dispositif de blocage de report 16 bloque le report C qui est émis en sortie depuis le circuit d'additionneur 15 et applique le report bloqué C sur le circuit d'additionneur 15 lors du cycle opératoire suivant.

L'unité de contrôleur 5 comprend un contrôleur arithmétique d'entiers 21 et un contrôleur arithmétique de champ fini GF (2^m) 22. L'unité de contrôleur 5 commande l'unité arithmétique 4 conformément à l'un de ces groupes de commande. Cette commutation de commande est réalisée conformément à une commande en provenance d'une CPU externe (par exemple la CPU de la figure 23).

Le contrôleur arithmétique d'entiers 21 commande l'unité arithmétique 4 de telle sorte qu'elle fonctionne en tant que multiplicateur basé sur les entiers longs. Dans ce but, le signal de commande S1 commande le sélecteur 13 afin d'émettre en sortie les données en provenance du circuit de multiplicateur basé sur les entiers 11 sur le circuit d'additionneur 14 et commande également les circuits d'additionneur 14 et 15 afin de faire en sorte qu'ils fonctionnent en tant

que circuit d'additionneur basé sur les entiers. Le contrôleur arithmétique d'entiers 21 exécute d'autres processus arithmétiques tels que les quatre opérations fondamentales de l'arithmétique en commandant le fonctionnement de l'unité arithmétique 4 en tant que multiplicateur basé sur les entiers.

Le contrôleur arithmétique de champ fini GF (2^m) 22 commande l'unité arithmétique 4 afin de la faire fonctionner en tant que multiplicateur basé sur champ fini GF (2^m). A cette fin, le signal de commande S1 commande le sélecteur 13 afin d'émettre en sortie les données émises en sortie depuis le circuit de multiplicateur basé sur les entiers 11 sur le circuit d'additionneur 14 et commande également les circuits d'additionneur 14 et 15 afin de faire en sorte qu'ils fonctionnent en tant que circuit d'additionneur basé sur champ fini GF (2^m). En outre, le contrôleur arithmétique de champ fini GF (2^m) 22 réalise des opérations d'addition et d'élévation au carré en commandant le fonctionnement de l'unité arithmétique 4 en tant que multiplicateur basé sur champ fini GF (2^m).

Afin de réaliser les processus respectifs qui sont décrits ci-avant, l'unité de contrôleur 5 commande les sections respectives en émettant en sortie un signal de commande S2.

Le fonctionnement de l'appareil arithmétique selon ce mode de réalisation qui présente l'agencement présenté ci-avant sera décrit ensuite.

Dans cet appareil arithmétique (le coprocesseur 1), le circuit de multiplicateur 12, le sélecteur 13 et similaire sont incorporés en tant qu'appareil de multiplicateur basé sur les entiers pour réaliser le traitement qui est à réaliser par un appareil de multiplicateur basé sur champ fini GF (2^m). Dans ce cas, conformément à un champ fini GF (2^m), un polynôme d'ordre (m-1) peut être exprimé en utilisant un vecteur de m bits comme suit :

$$a(x) = a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \ldots + a_1 x + a_0 \quad \ldots (1)$$
$$= [a_{m-1}, \cdots a_1, a_0]$$
$$b(x) = b_{m-1} x^{m-1} + b_{m-2} x^{m-2} + \ldots + b_1 x + b_0 \quad \ldots (2)$$

$= [b_{m-1}, \cdots b_1, b_0]$

Dans ce cas, une opération de multiplication basée sur champ fini GF (2^m) est une multiplication modulaire avec un polynôme irréductible d'ordre m f(x) sur GF (2^m) qui est établi en tant que module. En outre, un produit c(x) de 2 inconnues a(x) et b(x) de l'extension de champ de 2 est défini comme suit :

$$c(x) = a(x) \cdot b(x) \bmod f(x) \qquad (3)$$
$$= \Sigma\, a_k \cdot x^k \cdot b(x) \bmod f(x)$$
$$= c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \ldots + c_1 x + c_0$$
$$= [c_{m-1}, \cdots c_1, c_0]$$

En outre, un polynôme modulo f(x) peut être exprimé comme suit :

$$f(x) = f_m x^m + f_{m-1} x^{m-1} + \ldots + f_1 x + f_0 \qquad (4)$$
$$= [f_m, f_{m-1}, \cdots f_1, f_0]$$

Lors d'une opération de multiplication de polynôme basée sur champ fini GF (2^m) général, un registre à décalage basé sur une opération de décalage de cycle de multiplicateur est formé et un polynôme de reste après m décalages de cycle est établi en tant que résultat de multiplication. Cependant, selon ce mode de réalisation, ce traitement est réalisé en modifiant légèrement un circuit d'opération de produit-somme sur des nombres longs largement utilisé dans un LSI de traitement cryptographique basé sur les entiers.

Il est à noter que lorsque le coprocesseur 1 fonctionne en tant qu'appareil arithmétique basé sur les entiers conformément au signal de commande S1 en provenance de l'unité de contrôleur 5, cet appareil arithmétique fonctionne en tant que circuit d'opération de produit-somme sur des nombres longs. Dans ce circuit d'opération de produit-somme sur des nombres longs, le circuit de multiplicateur basé sur champ fini GF (2^m) calcule une équation (5) en tant que partie d'une opération de multiplication basée sur champ fini GF (2^m) suite à une commutation basée sur le signal de commande S1 :

$$c'(x) = a(x) \cdot b(x) \qquad \ldots(5)$$

Il est à noter que le circuit de multiplicateur basé sur champ fini GF (2^m) 12 ne calcule pas la partie "c(x)' mod f(x)" de l'équation (6) au niveau de l'étape de calcul de c'. C'est-à-dire que c' lui-même est calculé de la même manière que le produit de deux nombres lors d'une opération de multiplication basée sur les entiers en commutant seulement le circuit de multiplicateur 12 et les circuits d'additionneur 14 et 15 en utilisant le signal de commande S1.

Il est à noter que le multiplicateur de m bits et le multiplicande de c'(x) = a(x) · b(x) sont divisés selon des données de 32 bits et sont lus à partir de la mémoire et que le résultat d'opération est écrit dans la mémoire selon des unités de 32 bits. Le résultat d'opération final devient des données de 2m bits.

L'opération basée sur les entiers qui est réalisée par le circuit de multiplicateur basé sur les entiers 11 diffère de l'opération de polynôme basée sur champ fini GF (2^m) réalisée par le circuit de multiplicateur basé sur champ fini GF (2^m) en la présence/l'absence d'un report. Lors de l'opération basée sur les entiers, une expression logique d'addition est :

0 + 0 + Report (=0) = 0, Report = 0 ...(6)

1 + 0 + Report (=0) = 1, Report = 0

1 + 1 + Report (=0) = 0, Report = 1

De cette manière, l'opération doit considérer un report à partir d'un bit inférieur. A l'opposé de cela, dans un système algébrique basé sur champ fini GF (2^m), puisque chaque bit représente le coefficient de chaque terme d'un polynôme, aucune considération n'a besoin d'être apportée à un report jusqu'à un ordre différent.

En considération de ce qui précède, selon ce mode de réalisation, chaque unité arithmétique basée sur les entiers (multiplicateur ou additionneur) est commutée entre le mode normal qui permet une propagation de report et le mode exécution sans propagation de report. Dans ce cas, le mode inhibition (non exécution) de propagation de report est utilisé pour réaliser une opération arithmétique de champ fini GF (2^m). La dimension d'un circuit à

additionner pour commuter les modes de propagation de report est petite par comparaison avec la dimension de circuit totale.

Les figures 2A, 2B et 2C représentent un exemple de l'agencement d'un circuit arithmétique unitaire 4*4 bits qui met en œuvre c'(x) = a(x) . b(x).

Le circuit de multiplicateur basé sur champ fini GF (2^m) 12 de la figure 1 est obtenu en formant le dispositif d'opération unitaire représenté sur la figure 2A selon un agencement à 8*32 bits. Il est à noter que le circuit représenté sur la figure 2B correspond à une section d'entrée 29 du circuit de la figure 2A.

Les figures 3A, 3B, 3C et 3D représentent un exemple de l'agencement d'un circuit arithmétique unitaire 4*4 bits qui met en œuvre une opération de multiplication basée sur les entiers.

Le circuit de multiplicateur basé sur les entiers 11 représenté sur la figure 1 est obtenu en formant l'appareil arithmétique unitaire des figures 3A à 3D selon un agencement à 8*32 bits. La figure 3C représente l'agencement d'un additionneur complet FA qui est utilisé sur la figure 3A. La figure 3D représente l'agencement d'un report 31 de l'additionneur complet FA sur la figure 3C. La figure 3B représente une section d'entrée 30 du circuit de la figure 3A.

Dans l'appareil arithmétique de ce mode de réalisation, le circuit de multiplicateur basé sur champ fini GF (2^m) 12 et le circuit de multiplicateur basé sur les entiers 11 sont adjacents du point de vue logique l'un à l'autre et ces circuits 11 et 12 sont sélectionnés conformément au signal de commande S1 qui est généré depuis une commande d'opération arithmétique de champ fini GF (2^m) en provenance de l'unité de contrôleur 5, d'où la réalisation d'un traitement approprié.

Une sortie en provenance du sélecteur 13 est entrée sur le circuit d'additionneur 14. Dans ce cas, le circuit d'additionneur Z + (Y*X) 14 est un additionneur complet pour additionner des données de 40 bits (Y*X) et des données de 8 bits Z. Dans ce cas également, une addition basée sur champ fini GF (2^m) est réalisée en additionnant un

commutateur pour empêcher qu'un report du résultat obtenu en additionnant les bits respectifs ne soit propagé jusqu'à l'étage suivant conformément au signal de commande mentionné ci-avant.

La figure 4 est un schéma fonctionnel qui représente un exemple de l'agencement d'un additionneur complet du type report simultané 4bits comportant une fonction de commande de report qui est utilisé dans le coprocesseur de ce mode de réalisation.

Le circuit d'additionneur 14 représenté sur la figure 1 est obtenu en étendant l'additionneur complet présentant cet agencement selon un circuit capable d'additionner des données de 40 bits et des données de 8 bits.

Dans le circuit représenté sur la figure 4, des commutateurs 33 sont agencés entre les additionneurs complets 32 afin de commander la propagation de report.

La figure 5 représente un exemple de l'agencement d'un additionneur complet et d'un commutateur de commande de report qui sont utilisés dans le circuit d'additionneur selon ce mode de réalisation.

L'additionneur complet 32 et le commutateur 33 constituent un additionneur complet 42 comportant une fonction de commande de report pour un bit. Dans ce cas, l'additionneur complet 32 présente le même agencement que celui de l'additionneur complet FA de la figure 3C et le report 31 dans l'additionneur complet 32 présente le même agencement que celui du report de la figure 3D.

Le commutateur 33 qui est connecté à une ligne de propagation de report dans l'additionneur complet 32 est commandé par le signal de commande S1 en provenance de l'unité de contrôleur 5. Lorsqu'une opération basée sur des entiers doit être réalisée, le commutateur 33 est connecté. Lorsqu'une opération arithmétique de champ fini GF (2^m) doit être réalisée, le commutateur 33 est déconnecté.

La sortie (Z + (Y*X)) en provenance du circuit d'additionneur 14 présentant l'agencement mentionné ci-avant est propagée sur le circuit d'additionneur 15.

Le circuit d'additionneur C + Z + (Y*X) 15 au niveau du dernier étage du bloc d'opération arithmétique émet en sortie les 8 bits inférieurs des 40 bits en tant que résultat de multiplication en tant que données R et additionne les 32 bits supérieurs à Z + (Y*X) lors du cycle suivant.

De façon similaire au circuit d'additionneur 14, le circuit d'additionneur 15 est un additionneur complet comportant une fonction de commande de report représentée sur la figure 4, comme commandé par le signal de commande S1. Par conséquent, dans le mode opération basée sur les entiers, le circuit d'additionneur 15 joue le rôle d'additionneur complet réglé sur le LSB (le bit le plus faible) afin d'exécuter une addition basée sur les entiers. Dans le mode opération arithmétique de champ fini GF (2^m), le circuit d'additionneur 15 exécute une addition basée sur champ fini GF (2^m).

Les données de sortie R en provenance du circuit d'additionneur 15 sont stockées temporairement dans la mémoire 2 par l'intermédiaire du bus de données 3. Ces données deviennent les données Z à nouveau et elles retournent au coprocesseur 1 et une opération de multiplication basée sur les entiers ou une opération de multiplication basée sur champ fini GF (2^m) est poursuivie. Cette opération est répétée le nombre de fois qui correspond au nombre requis de cycles, d'où ainsi l'obtention d'un résultat de multiplication.

Dans ce cas, le résultat de l'équation (5) peut être obtenu conformément à une commande de multiplication basée sur champ fini GF (2^m), et une opération de multiplication basée sur champ fini GF (2^m) est terminée par une multiplication modulaire avec le polynôme irréductible f(x) en tant que module comme défini par l'équation (6). De façon similaire à une division sur le papier, la multiplication modulaire peut être réalisée en répétant le traitement constitué par l'acquisition d'un quotient à partir des chiffres supérieurs d'un dividende et par la soustraction du dividende courant du produit du quotient courant et d'un diviseur (dans un champ d'extension 2, la soustraction et l'addition sont réalisées de la même manière) le nombre de fois correspondant au

nombre requis de cycles. Ce traitement peut être réalisé en exécutant une commande de multiplication basée sur champ fini GF (2^m) et une commande d'addition (cette opération sera décrite en détail selon le troisième mode de réalisation). Une opération d'élévation au carré basée sur champ fini GF (2^m) peut être réalisée au moyen du même traitement que celui pour une opération de multiplication. Une opération d'inversion peut être réalisée en répétant de façon mutuelle des opérations de multiplication et d'élévation au carré.

Un cas selon lequel l'unité arithmétique 4 fonctionne en tant qu'additionneur basé sur champ fini GF (2^m) conformément à une commande d'addition basée sur champ fini GF (2^m) sera décrit ci-après.

De façon similaire à une addition de polynôme générale, l'addition basée sur champ fini GF (2^m) est réalisée en additionnant les coefficients du même ordre comme suit :

$$c(x) = a(x) + b(x) \quad \ldots(7)$$
$$= [a_{m-1} + b_{m-1}, a_{m-2} + b_{m-2}, \cdots, a_0 + b_0]$$

Dans ce cas, la somme des coefficients des ordres respectifs est 0 + 0 = 1 + 1 = 0 et 0 + 1 = 1 + 0 = 1, et il s'ensuit qu'aucun report n'est produit à la différence d'une addition basée sur les entiers. Par conséquent, une addition basée sur champ fini GF (2^m) peut être de façon générale mise en œuvre au moyen de m portes OU-exclusif.

Dans un appareil de multiplicateur basé sur les entiers, une addition peut être traitée en tant que c = b + a*1. Selon ce mode de réalisation, par conséquent, une addition basée sur champ fini GF (2^m) est également exécutée en tant que c(x) = b(x) + a(x) * 1 en utilisant cet algorithme sans de quelconques modifications. Cette opération arithmétique peut être réalisée en réalisant une commutation sur la base du signal de commande S1 du fait que les additionneurs complets représentés sur la figure 4 sont utilisés pour les circuits d'additionneur 14 et 15.

En outre, lors de la commutation d'une opération en utilisant le signal de commande S1, le coprocesseur 1 devient un circuit qui

dispose de la même fonction que celle du coprocesseur représenté sur la figure 4, d'où la réalisation d'une opération basée sur les entiers également.

Comme décrit ci-avant, dans l'appareil arithmétique selon ce mode de réalisation de la présente invention, le dispositif de multiplicateur basé sur les entiers inclut le dispositif de multiplicateur unitaire pour une opération de multiplication basée sur les entiers et le dispositif arithmétique unitaire pour une opération de multiplication basée sur champ fini GF (2^m), qui présente un agencement de circuit similaire à celui de l'appareil de multiplicateur unitaire, et une commande d'opération arithmétique de champ fini GF (2^m) est additionnée à une commande de multiplication basée sur les entiers. En outre, cet appareil inclut le sélecteur commandé par un signal de commande qui est généré à partir d'une commande arithmétique de champ fini GF (2^m) et le commutateur pour commander la propagation d'un report en sortie de chaque bit de l'additionneur complet. L'appareil arithmétique de la présente invention peut par conséquent exécuter à la fois une opération basée sur les entiers et une opération arithmétique de champ fini GF (2^m) sans utiliser un quelconque dispositif de multiplicateur basé sur champ fini GF (2^m) séquentiel qui utilise un registre à décalage classique.

Un accélérateur de traitement cryptographique par clé publique permettant d'exécuter des opérations d'addition et de multiplication basées sur champ fini GF (2^m) en utilisant un circuit d'opération de produit–somme sur des nombres longs peut par conséquent être constitué en additionnant de petits nombres d'instructions et de circuits en tant que fonctions d'extension additionnelles à une unité arithmétique basée sur les entiers classique. Il est à noter que la dimension de circuit requise pour réaliser ce mode de réalisation est faible par comparaison avec la dimension de circuit totale.

Conformément à l'appareil de traitement cryptographique de ce mode de réalisation, un LSI comportant des fonctions abondantes permettant de manipuler le système cryptographique à courbe elliptique

basé sur champ fini GF (2^m) ainsi que le système RAS basé sur les entiers peut être constitué en tant que coprocesseur de traitement cryptographique sans augmenter de façon spécifique l'aire de mise sous module. Un appareil de cryptage/décryptage permettant de manipuler à la fois un système cryptographique RAS et un système cryptographique à courbe elliptique peut être mis en œuvre même dans un appareil disposant d'une aire de mise sous module faible, tel qu'une carte IC.

Les additionneurs complets qui disposent de fonctions de commande de report et qui constituent les circuits d'additionneur 14 et 15 représentés sur la figure 4 seront décrits.

La figure 6 représente un autre additionneur complet disposant d'une fonction de commande de report.

Tout comme le circuit de la figure 5, cet additionneur complet 43 disposant de la fonction de commande de report comprend un commutateur 33 et un additionneur complet 32. Cependant, dans le circuit de la figure 6, le commutateur 33 est prévu sur le coté d'entrée d'un report 31 à la différence du circuit de la figure 5 dans lequel le commutateur 33 est prévu sur le coté de sortie du report 31.

La figure 7 représente encore un autre additionneur complet comportant une fonction de commande de report.

Cet additionneur complet 44 disposant de la fonction de commande de report réalise une commande de report en commandant la sélection d'un résultat d'addition en tant que sortie. De façon davantage spécifique, un commutateur 33' est un sélecteur qui sélectionne une sortie en provenance d'une porte OU-exclusif 35 ou d'une porte OU-exclusif 36 sur la base du signal de commande S1. Un additionneur complet du type report simultané obtenu en connectant ces additionneurs complets peut commander une propagation de report conformément au signal de commande S1.

On suppose que le signal de commande S1 de la figure 7 est un signal de commande qui est basé sur une commande d'opération arithmétique de champ fini GF (2^m). Dans ce cas, si le signal S1 vaut

"1", des sorties a et b en provenance de la porte OU-exclusif 35 deviennent des résultats d'opération. En tant que conséquence, l'additionneur complet 44 fonctionne en tant qu'additionneur basé sur champ fini GF (2^m). Si le signal S1 vaut "0", une sortie en provenance de l'additionneur complet 44 devient un résultat d'opération. En tant que conséquence, l'additionneur complet 44 fonctionne en tant qu'additionneur basé sur les entiers.

(Second mode de réalisation)

La figure 8 représente un exemple de l'agencement d'un appareil arithmétique selon le second mode de réalisation de la présente invention. Les mêmes index de référence que sur la figure 1 représentent les mêmes parties sur la figure 8 et leur description sera omise. Seulement les parties différentes seront décrites ci-après. Il est à noter qu'une description répétitive sera évitée dans chaque mode de réalisation décrit ci-après.

Un coprocesseur 1' en tant que cet appareil arithmétique présente le même agencement que celui selon le premier mode de réalisation à ceci près qu'il comporte un circuit de multiplicateur 41 en lieu et place du circuit de multiplicateur basé sur les entiers 11, du circuit de multiplicateur basé sur champ fini GF (2^m) 12 et du sélecteur 13 de la figure 1.

Ce circuit de multiplicateur 41 est conçu pour commuter le mode multiplication basé sur les entiers et le mode multiplication basé sur champ fini GF (2^m) (seulement c' au niveau de l'équation (6)) conformément à un signal de commande S1 en provenance d'une unité de contrôleur 5.

Les figures 9A et 9B représentent un exemple de l'agencement d'un circuit arithmétique unitaire 4*4 bits permettant de réaliser le circuit de multiplicateur de ce mode de réalisation. Dans la pratique, le circuit de multiplicateur 41 est réalisé en formant le dispositif arithmétique unitaire représenté sur les figures 9A et 9B selon un dispositif présentant une configuration 8*32 bits. Le circuit de la figure 9B représente une section d'entrée 29 du circuit de la figure 9A.

Comme représenté sur la figure 9A, le circuit de multiplicateur 41 utilise l'additionneur complet 42 comportant la fonction de commande de report selon la figure 5 en tant qu'additionneur complet et il s'ensuit qu'il peut commander la propagation de report conformément au signal de commande S1. La commutation du mode multiplication basée sur les entiers et du mode multiplication basée sur champ fini GF (2^m) peut être réalisée au moyen d'une commande d'opération arithmétique de champ fini GF (2^m).

L'appareil arithmétique de ce mode de réalisation peut par conséquent fonctionner d'une manière similaire à celle du premier mode de réalisation.

Comme décrit ci-avant, l'appareil arithmétique et l'appareil de traitement cryptographique selon ce mode de réalisation de la présente invention utilisent le circuit de multiplicateur 41 en lieu et place du circuit de multiplicateur basé sur les entiers 11, du circuit de multiplicateur basé sur champ fini GF (2^m) 12 et du sélecteur 13 et mettent en œuvre les fonctions des circuits 11, 12 et 13 en utilisant un seul circuit 41. En plus d'effets similaires à ceux du premier mode de réalisation, ce mode de réalisation peut réaliser un commutation entre l'opération de multiplication basée sur les entiers et l'opération de multiplication basée sur champ fini GF (2^m) en utilisant moins de circuits additionnels.

Selon ce mode de réalisation, l'additionneur complet représenté sur la figure 5 est utilisé en tant qu'additionneur complet 42 comportant la fonction de commande de report. Cependant, l'additionneur complet 43 ou 44 comportant une fonction de commande de report représenté sur la figure 6 ou 7 peut être utilisé en lieu et place de l'additionneur complet 42 comportant une fonction de commande de report.

(Troisième mode de réalisation)

La figure 10 est un schéma fonctionnel qui représente un exemple de l'agencement d'un coprocesseur appliqué à un appareil arithmétique et à un appareil de traitement cryptographique selon le troisième mode de réalisation de la présente invention.

Ce mode de réalisation est un exemple concret de la section modulo du premier mode de réalisation. Comme représenté sur la figure 10, une unité de contrôleur 5 inclut un contrôleur arithmétique de champ fini GF (2^m) 22a comportant une fonction modulo additionnée à la fonction mentionnée ci-avant et un circuit d'acquisition de quotient 50 qui est commandé par la fonction modulo et qui comporte une section de calculateur d'inverse 51.

Dans ce cas, en plus de la fonction mentionnée ci-avant consistant à commander une unité arithmétique 4 pour obtenir un résultat de multiplication c'(x) de l'équation (5), le contrôleur arithmétique de champ fini GF (2^m) 22a dispose de la fonction consistant à commander l'unité arithmétique 4 et le circuit d'acquisition de quotient 50 pour exécuter un modulo pour ce résultat de multiplication c'(x) en utilisant un polynôme modulo f(x). Plus spécifiquement, la fonction de commande inclut la fonction consistant à entrer/émettre en sortie des données sur/depuis une mémoire 2 et des tampons 17X, 17Y, 17Z et 17R sur la base de l'algorithme opératoire qui sera décrit ultérieurement et la fonction consistant à générer diverses commandes telles qu'une commande de multiplication, une commande d'addition et une commande d'opération d'inversion et à les appliquer sur des circuits arithmétiques correspondants conformément à l'opération d'entrée/sortie.

Le circuit d'acquisition de quotient 50 est utilisé pour calculer un quotient en divisant le polynôme de dividende c'(x) par le polynôme de modulo f(x) en tant que partie d'un modulo. Dans ce cas, le circuit d'acquisition de quotient 50 dispose de la fonction consistant à obtenir le quotient mentionné ci-avant en multipliant un inverse $\beta(x)$ du polynôme modulo f(x) et le polynôme de dividende c'(x).

Plus spécifiquement, le circuit d'acquisition de quotient 50 est commandé par le contrôleur arithmétique de champ fini GF (2^m) 22a et il dispose de la fonction consistant à appliquer les deux blocs supérieurs ($F_{L-1(x)}$, $F_{L-2(x)}$) du polynôme modulo f(x) dans la mémoire 2 sur la section de calculateur d'inversion 51 seulement à un instant du

modulo et à faire en sorte que la section 51 calcule l'inverse $\beta(x)$ des deux blocs supérieurs, de la fonction consistant à lire l'inverse obtenu $\beta(x)$ à partir de la mémoire 2 lorsque l'inverse est écrit dans la mémoire 2, de la fonction consistant à obtenir un quotient $\gamma(x)$ en multipliant l'inverse lu $\beta(x)$ et les deux blocs supérieurs ($C'_{L-1(x)}$, $C'_{L-2(x)}$) du polynôme de dividende courant, de la fonction consistant à établir le quotient obtenu $\gamma(x)$ en tant que quotient qi(x) des deux blocs supérieurs et à écrire le quotient qi(x) dans la mémoire 2 et de la fonction consistant à répéter l'opération à partir de la lecture de l'inverse $\beta(x)$ jusqu'à l'écriture du quotient qi(x) jusqu'à ce qu'un reste c(x) soit obtenu, comme représenté sur la figure 11.

Comme représenté sur la figure 13, la section de calculateur d'inverse 51 dispose de la fonction consistant à calculer l'inverse $\beta(x)$ des deux blocs supérieurs ($F_{L-1(x)}$, $F_{L-2(x)}$) du polynôme modulo f(x) dans la mémoire 2 suite à la réception des deux blocs ($F_{L-1(x)}$, $F_{L-2(x)}$) en provenance du circuit d'acquisition de quotient 50 comme représenté sur la figure 12 et de la fonction consistant à écrire l'inverse obtenu $\beta(x)$ dans la mémoire 2. Le LFSR représenté sur la figure 27 est utilisé en tant que circuit de division en tant que partie de la section de calculateur d'inverse 51.

Dans ce cas, l'inverse $\beta(x)$ comporte un nombre fixe de bits et n'est pas un simple inverse mais est corrigé à l'avance comme représenté sur la figure 13 afin d'éliminer la nécessité de normaliser un diviseur et de dénormaliser un résultat d'opération lors de l& multiplication modulaire principale qui suit. En outre, l'inverse $\beta(x)$ lui-même peut être calculé par l'unité arithmétique 4 en lieu et place du circuit d'acquisition de quotient 50 incluant la section de calculateur d'inverse 51.

Si par exemple la largeur de bus d'un circuit d'opération de produit-somme basée sur les entiers est aussi faible que 8 bits, la section de calculateur d'inverse 51 peut être remplacée par un schéma consistant à stocker les inverses de toutes les valeurs de 8 bits en tant que table dans une ROM ou similaire. Cependant, si la largeur du bus

est de 16 bits ou plus, la section de calculateur d'inverse 51 est davantage préférable que le schéma consistant à stocker les inverses de toutes les valeurs de 16 bits dans une ROM en considération de la réduction des coûts.

Le fonctionnement de l'appareil arithmétique (coprocesseur) présentant l'agencement mentionné ci-avant sera décrit ensuite.

Lors d'une multiplication modulaire pour une base de polynôme basé sur champ fini GF (2^m) conformément à la présente invention, une opération de multiplication et un modulo sont réalisés séparément. Plus spécifiquement, comme représenté sur la figure 14, des polynômes a(x) et b(x) en tant que multiplicande/multiplicateur et un polynôme modulo f(x) sont entrés comme représenté sur la figure 14 (étape ST1) et une opération de multiplication de a(x) . b(x) est réalisée afin d'obtenir un résultat de multiplication $C'_{(x)}$ présentant une longueur binaire double (étape ST2). Un modulo $C'_{(x)mod}$ f(x) est ensuite réalisé (étape ST3) afin d'obtenir un reste c(x) (étape ST4).

L'opération de multiplication de l'étape ST2 est réalisée de la même manière que selon les premier et second modes de réalisation. Le modulo des étapes ST3 et ST4 sera décrit ci-après. Le calcul sur le papier sera décrit en premier et un processus réel correspondant à un calcul sur papier sera ensuite décrit.

Comme indiqué par le calcul sur papier sur la figure 15, un modulo pour l'équation (6) est réalisé après que le diviseur f(x) et le dividende c'(x) sont divisés selon des blocs unitaires dont chacun est constitué par un nombre prédéterminé k de bits. Il est à noter que, par exemple, le nombre de bits de chaque bloc unitaire peut être établi en correspondance avec la largeur de bus du coprocesseur 1.

Un bloc supérieur c'L-i(x) du dividende c'(x) est divisé par f(x) et un quotient qi(x) d'un bloc est acquis à partir du chiffre supérieur. Une opération qui est c'(x) – f(x) . qi(x) est ensuite réalisée afin de soustraire le dividende c'(x) d'un bloc à partir du chiffre supérieur.

Plus spécifiquement, chaque fois que le quotient qi(x) d'un bloc est multiplié par le polynôme de diviseur f(x), (m + 1) blocs sont obtenus

en tant que résultat de multiplication. Ce résultat de multiplication est soustrait (= est additionné) du polynôme de dividende courant c'(x) afin de calculer le polynôme de dividende suivant de (2m – 1 * n) blocs (n est le nombre de fois d'opérations de multiplication). C'est-à-dire que le dividende précédent c'(x) est diminué selon des unités de blocs.

Un modulo est terminé en répétant ce traitement depuis l'acquisition d'un quotient jusqu'à la soustraction du quotient n fois (= le nombre de bits d'un dividende/le nombre de bits de chaque bloc unitaire) et en obtenant le reste c(x).

Un traitement réel pour un modulo sera décrit ensuite.

Lors du modulo mentionné ci-avant, le circuit d'acquisition de quotient 50 acquiert le quotient qi(x) comme représenté sur la figure 11 et l'unité arithmétique 4 diminue le dividende c'(x) en calculant c'(x) – f(x) . qi(x) comme représenté sur la figure 16. Les opérations du circuit d'acquisition de quotient 50 et de l'unité arithmétique 4 seront décrites séquentiellement ci-après.

Lors du calcul du premier quotient, le circuit d'acquisition de quotient 50 lit les deux blocs supérieurs ($F_{L-1}(x)$, $F_{L-2}(x)$) du diviseur f(x) à partir de la mémoire 2 et entre ceux-ci sur la section de calculateur d'inverse 51 afin de calculer l'inverse $\beta(x)$ du diviseur f(x), comme représenté sur les figures 11 et 12.

Comme représenté sur la figure 13 et au niveau de l'équation (8), la section de calculateur d'inverse 51 stocke un nombre $\underline{d}$ de chiffres 0 consécutifs à partir du bit de poids le plus fort MSB du bloc supérieur $F_{L-1}(x)$ des deux blocs ($F_{L-1}(x)$, $F_{L-2}(x)$) comme donné par :

$$d = \text{count\_zero}(F_{L-1}(x)) \quad \ldots(8)$$

où count_zero() est une fonction de comptage du nombre de 0 consécutifs à partir du MSB de la valeur de ().

La section de calculateur d'inverse 51 calcule également un nombre $\underline{h}$ de chiffres d'un décalage à gauche (comme décrit ultérieurement) sur la base de ce nombre $\underline{d}$ de chiffres invalides selon :

$$h = (d+1) \bmod k \quad \ldots(9)$$

et le stocke.

Comme représenté sur la figure 13 et au niveau de l'équation (10), la section de calculateur d'inverse 51 calcule un inverse $\alpha(x)$ des deux blocs supérieurs ($F_{L-1}(x)$, $F_{L-2}(x)$) du diviseur $f(x)$ en utilisant un LFSR 90 comme suit :

$$\alpha(x) = x^{2k} / (F_{L-1}(x) \cdot X^{k} + F_{L-2}(x)) \quad \ldots(10)$$

Le cas dans lequel un bloc est constitué par 16 bits ($k = 16$) sera décrit. On suppose également qu'un dividende vaut x^{2*16} ($= x^{2k}$) dont le bit de poids le plus fort MSB vaut "1" et dont les autres bits sont à "0".

Après établissement des deux blocs supérieurs ($F_{L-1}(x)$, $F_{L-2}(x)$) en tant que diviseur dans une unité de coefficient 93 sur la figure 27, la section de calculateur d'inverse 51 entre le dividende x^{2i} sur le registre à décalage depuis les ordres plus élevés et répète un décalage selon des unités d'horloges 2*16 fois, d'où ainsi l'obtention d'un inverse de 32 bits $\alpha(x)$. Il est à noter qu'un bloc peut être constitué par 8 ou 32 bits ou par tout autre nombre arbitraire de bits. Dans un tel cas également, l'inverse $\alpha(x)$ peut être calculé au moyen du même schéma.

Ensuite, la section de calculateur d'inverse 51 concatène les "0" des (k-1) bits et le "1" d'un bit pour le MSB de cet inverse $\alpha(x)$ afin d'obtenir une valeur de 2k-bits $\alpha'(x)$. La section de calculateur d'inverse 51 décale ensuite cette valeur de 2k-bits $\alpha'(x)$ vers la gauche du nombre h de chiffres du décalage vers la gauche comme obtenu au niveau de l'équation (9) afin de calculer l'inverse corrigé $\beta(x)$:

$$\beta(x) = \alpha'(x) \cdot x^{h} \quad \ldots(11)$$

Dans ce cas, l'inverse corrigé $\beta(x)$ est une valeur qui satisfait les équations (8) à (11) mentionnées ci-avant. L'inverse $\beta(x)$ est calculé seulement une fois en relation avec le polynôme modulo appliqué $f(x)$ et est stocké dans la mémoire 2 et est lu à partir de la mémoire 2 par la suite. Même si le dividende change, l'inverse $\beta(x)$ reste le même aussi longtemps que le polynôme modulo $f(x)$ reste le même. Pour cette raison, l'inverse $\beta(x)$ peut être lu à partir de la mémoire 2 sans calculer un quelconque nouvel inverse.

Lors d'un calcul de quotient, si l'inverse $\beta(x)$ est établi à l'avance, un modulo peut être exécuté au moyen des équations (12) à (15) présentées ci-après.

Comme indiqué par l'équation (12) et par la figure 11, le circuit d'acquisition de quotient 50 multiplie les deux blocs supérieurs ($C'_{L-1}(x)$, $C'_{L-2}(x)$) d'un dividende courant C'i ($0 <= i <= n$) et l'inverse $\beta(x)$:

$$\gamma(x) = \beta(x) . (C'_{L-1}(x) . x^{k} + C'_{L-2}(x)) \quad ...(12)$$

En outre, comme indiqué par l'équation (13), le circuit d'acquisition de quotient 50 extrait un chiffre correspondant à un quotient qi(x) d'un bloc en tant que second bloc supérieur à partir d'un résultat $\gamma(x)$ comme suit :

$$qi(x) = \gamma(x) / x^{2k} \quad ...(13)$$

et l'écrit dans la mémoire 2. Par conséquent, le quotient qi(x) d'un bloc est obtenu.

Comme représenté sur la figure 16, l'unité arithmétique 4 soustrait un produit f(x) . qi(x) du diviseur et du quotient à partir du dividende courant c'i(x).

Plus spécifiquement, dans l'unité arithmétique 4, un circuit de multiplicateur basé sur champ fini GF (2^m) 12 multiplie le polynôme modulo f(x) et le quotient qi(x) du bloc courant afin d'obtenir un résultat de multiplication P(x) :

$$P(x) = f(x) . qi(x) \quad ...(14)$$

Des circuits d'additionneur 14 et 15 soustraient (= additionnent) ce résultat de multiplication P(x) du dividende courant C'i afin d'obtenir un dividende suivant C'i+1 :

$$C'i+1 = C'i + P(x) \quad ...(15)$$

Les équations (12) à (15) sont calculées de façon répétée n fois afin d'obtenir pour finir un reste c(x) comme représenté sur les figures 14 à 16. Ce reste c(x) (= $[c_{m-1}, ..., c_1, c_0]$) correspond au résultat de multiplication modulaire final c(x) indiqué par l'équation (3).

A l'aide du traitement présenté ci-avant, le résultat de multiplication modulaire c(x) représenté par l'équation (6) peut être calculé à partir du résultat de multiplication c'(x) représenté par

l'équation (5) comme décrit selon le premier ou le second mode de réalisation, ce qui termine un modulo défini par une multiplication et une multiplication modulaire.

(Evaluation)

Les vitesses de traitement et les dimensions de circuit des coprocesseurs 1 des premier à troisième modes de réalisation qui réalisent des multiplications modulaires selon la manière présentée ci-avant ont été évaluées. Des résultats d'évaluation seront décrits séquentiellement ci-après.

(Evaluation de la vitesse de traitement)

La figure 17 représente le nombre requis d'horloges de commande dans le coprocesseur 1 lorsque m (nombre de bits) = 160 et m = 1024. Lorsque ce coprocesseur est appliqué au système cryptographique à courbe elliptique, m (nombre de bits) = 160 est une dimension typique. Dans le cas de m = 1024 de la figure 17, puisque la longueur de clé maximum qui est présentement considérée en tant que valeur optimum dans le système cryptographique RSA basé sur les entiers est de 1024 bits, les valeurs de la figure 17 sont présentées en tant qu'estimations de vitesse en considération d'une augmentation attendue de la longueur de clé d'un système de cryptographie à courbe elliptique.

Pour une comparaison entre les vitesses de traitement, les nombres d'horloges de traitement au niveau des opérations d'addition, de multiplication et d'élévation au carré d'une extension de champ GF de 2 (2^{160}) de 160 bits ont étés évalués. La figure 18 représente les résultats. Il est à noter que les nombres d'horloges au niveau des opérations d'addition, d'élévation au carré et de multiplication incluent les nombres d'horloges basés sur un modulo en utilisant un polynôme modulo à la différence du cas représenté sur la figure 17 par souci de comparaison avec la vitesse d'une opération GF (2^{160}).

Chaque rapport SR en tant que valeur de comparaison est obtenu en divisant le nombre de blocs dans le coprocesseur 1 par le nombre d'horloges dans un circuit de registre à décalage général. Plus

cette valeur est faible, plus la vitesse de traitement est élevée. Conformément à ces rapports SR, le coprocesseur 1 de la présente invention peut exécuter des opérations arithmétiques de champ fini GF (2^m) à l'exclusion d'une opération d'addition à une vitesse de traitement égale ou supérieure à celle du circuit de registre à décalage général.

(Evaluation de la dimension de circuit)

Comme représenté sur la figure 19, la dimension de circuit totale du coprocesseur 1 correspond à environ 30k portes. Le circuit du coprocesseur 1 est formé en additionnant le circuit pour traiter une opération arithmétique de champ fini GF (2^m) à un coprocesseur basé sur les entiers.

De façon davantage spécifique, comme représenté sur la figure 20, dans l'unité arithmétique 4, le circuit de commutation de report est additionné au circuit d'opération de produit-somme. Dans l'unité de contrôleur 5, le circuit d'acquisition de quotient 50 est additionné pour une opération de division bien qu'il soit simplement requis d'additionner de quelconques circuits pour des opérations d'addition, de multiplication et d'élévation au carré. Aucune RAM (la mémoire 2) ni I/F (interface) n'ont besoin d'être ajoutés du fait que ces éléments sont partagés avec le coprocesseur basé sur les entiers.

La dimension de circuit totale des circuits additionnels est d'environ 5k portes. La dimension des circuits additionnels de 5k portes n'est pas très importante pour la technologie LSI récente. C'est-à-dire que cette dimension tombe dans la plage dans laquelle le coprocesseur 1 de la présente invention peut être utilisé de façon satisfaisante en lieu et place du coprocesseur existant.

A titre de comparaison, les dimensions de circuit de coprocesseurs conçus spécifiquement pour des opérations arithmétiques de champ fini GF (2^m) ont étés estimées lorsque des fonctions d'opération arithmétique de champ fini GF (2^m) (des opérations d'addition, de multiplication et d'élévation au carré) ont été

réalisées sans utiliser le coprocesseur 1 de la présente invention. La figure 21 représente les résultats.

Comme représenté sur la figure 21, lorsque m = 160, la dimension de circuit du coprocesseur conçu spécifiquement pour des opérations arithmétiques de champ fini GF (2^m) est de 10k portes. Lorsque m = 1024, cette dimension devient égale à 16k portes. Bien évidemment, par conséquent, des fonctions d'opération arithmétique de champ fini GF (2^m) peuvent être réalisées par le coprocesseur 1 de la présente invention moyennant une dimension des circuits additionnels qui est égale à entre environ la moitié et un tiers de celle requise lorsque le coprocesseur conçu spécifiquement pour des opérations arithmétiques de champ fini GF (2^m) est utilisé.

Comme décrit ci-avant, selon ce mode de réalisation, en plus des effets du premier mode de réalisation, les effets qui suivent peuvent être obtenus. Puisque le circuit d'opération de produit-somme sur des nombres longs réalise une opération arithmétique selon un modulo en lieu et place du registre à décalage à retour linéaire LFSR 90, un degré arbitraire m qui est égal ou supérieur à l'unité peut être utilisé. Même si le degré m d'un champ fini GF (2^m) augmente, une opération arithmétique peut être exécutée sans modifier l'appareil. En outre, l'élimination de restrictions en termes de composants matériels du fait des limitations qui pèsent sur le degré m permet à l'appareil de faire face de façon appropriée à une augmentation du nombre de bits d'une clé de cryptage.

En outre, puisqu'une multiplication modulaire basée sur champ fini GF (2^m) est divisée selon un traitement de multiplication et un modulo (division) pour permettre l'utilisation d'un polynôme modulo arbitraire f(x), la versatilité générale peut être améliorée.

Lors d'un modulo, lorsque le circuit d'acquisition de quotient 50 calcule un quotient sur la base du polynôme de dividende c'(x) et du polynôme de diviseur f(x) afin d'acquérir un polynôme de quotient qi(x) d'un bloc moyennant le nombre de bits correspondant à la largeur de bus à partir des ordres plus élevés, l'unité arithmétique 4 calcule le

polynôme de dividende suivant c'i-1(x) en soustrayant le résultat de multiplication qi(x) . f(x) du polynôme de quotient qi(x) et du polynôme de diviseur f(x) à partir du polynôme de dividende courant c'i(x).

Le coprocesseur 1 obtient le reste c(x) en répétant ce traitement, depuis le calcul du quotient en utilisant le circuit d'acquisition de quotient 50 jusqu'au calcul des données de polynôme de dividende au moyen de l'opération de produit-somme en utilisant l'unité arithmétique 4. Ceci rend possible de réaliser un modulo efficient et un calcul de quotient efficient en utilisant les caractéristiques des composants matériels.

Lors d'un calcul de quotient, le circuit d'acquisition de quotient 50 multiplie les données d'inverse des deux blocs supérieurs des données de polynôme de diviseur et des deux blocs supérieurs des données de polynôme de dividende courant et établit le second bloc supérieur du résultat de multiplication en tant que données de polynôme de quotient d'un bloc. Le circuit d'acquisition de quotient 50 peut extraire une partie de nombre effective à partir du polynôme de quotient obtenu. Par conséquent, la précision de l'opération peut être optimisée.

Lors d'un calcul de quotient, une commande indépendante est établie pour calculer l'inverse $\beta(x)$ à partir des deux blocs supérieurs du polynôme de diviseur f(x), et l'inverse $\beta(x)$ est calculé avant une opération arithmétique de champ fini GF (2^m). L'inverse obtenu $\beta(x)$ est stocké dans la mémoire 2. Lors de l'exécution d'un modulo, l'inverse $\beta(x)$ est lu à partir de la mémoire 2.

Lors de l'exécution d'un modulo redondant sous le même polynôme modulo, un quotient est acquis en lisant les données d'inverse à partir de la mémoire et il s'ensuit que le temps requis pour calculer les données d'inverse peut être économisé lors du second calcul de quotient et des calculs de quotient qui suivent. Ceci permet de raccourcir le temps de traitement pour une opération d'élévation au carré et de multiplication (multiplication modulaire) basée sur champ fini GF (2^m). En outre, puisque l'inverse $\beta(x)$ peut être calculé à l'avance,

une multiplication modulaire basée sur champ fini GF (2^m) peut être réalisée en utilisant seulement le circuit d'opération de produit-somme pour réaliser des opérations de multiplication et d'addition.

Lors du calcul des données d'inverse, le circuit d'acquisition de quotient 50 compte le nombre de 0 consécutifs à partir des bits d'ordre élevé des deux blocs supérieurs des données de polynôme de diviseur et extrait des données de polynôme de 1 bloc + 1 bit à partir des bits d'ordre élevé de telle sorte que le bit de poids le plus fort soit établi à 1. Le circuit d'acquisition de quotient 50 obtient l'inverse des données de polynôme extraites et concatène les données corrigées de 1 bloc dont le bit de poids le plus faible est "1" et dont les autres bits sont 0 avec le bit de poids le plus fort de l'inverse obtenu de manière à obtenir de façon globale des données de deux blocs. Le circuit d'acquisition de quotient 50 décale ensuite du point de vue des bits ces données en direction du côté d'ordre élevé d'une valeur correspondant au comptage des 0 et établit les données résultantes en tant que données d'inverse.

Une valeur corrigée est établie en tant que données d'inverse pour éviter la normalisation d'un diviseur, une correction d'un quotient approché et une dé-normalisation de résultats d'opération tels qu'un quotient et qu'un reste, comme réalisé sur la base de l'algorithme de Knuth à l'aide d'une opération de division simple précision qui est utilisée lors d'une opération de division basée sur des entiers longs générale. Ceci rend possible de diminuer le nombre des décalages de bits et d'optimiser l'appareil arithmétique.

Lors d'une opération de multiplication basée sur des entiers, par exemple, m bits * m bits = 2m bits de telle sorte que même si des 0 consécutifs sont agencés en tant que plusieurs bits supérieurs des 2m bits, le nombre des bits effectifs est de 2m. Si une opération de division (modulo) doit être réalisée en utilisant ce résultat de multiplication, puisqu'une opération de division ne peut pas être réalisée en utilisant 0, un diviseur et un dividende doivent être décalés vers la gauche pour être normalisés à l'avance de telle sorte que 1 soit établi en tant que MSB. Lorsque l'opération est terminée après une boucle prédéterminée,

le résultat d'opération (quotient et reste) doit également être dénormalisé en étant décalés vers la droite du nombre de bits dont le diviseur et le dividende ont été décalés vers la gauche.

Selon ce mode de réalisation, puisqu'un diviseur (données d'inverse β(x)) lors d'une opération de quotient est corrigé pour éliminer la nécessité d'un traitement avant et après une telle boucle de division, l'appareil arithmétique peut être optimisé.

Selon ce mode de réalisation, puisqu'une opération arithmétique est exécutée selon des unités de blocs au lieu de l'être selon des unités de bits en utilisant l'inverse corrigé β(x), le nombre de décalages de bits peut être diminué et la vitesse de traitement peut être augmentée.

En outre, un appareil arithmétique et un appareil de cryptage/décryptage peuvent être réalisés moyennant une faible quantité de circuits additionnels dont chacun incorpore un LSI qui fonctionne à une vitesse de traitement égale ou supérieure à celle d'un circuit de multiplicateur basé sur champ fini GF (2^m) du type registre à décalage général moyennant un nombre faible de commandes et un système arithmétique qui utilise un circuit d'opération de produit-somme sur des nombres longs et ils peuvent exécuter divers systèmes cryptographiques sur la base d'une opération basée sur les entiers et d'une opération arithmétique de champ fini GF (2^m). En tant que système cryptographique qui utilise une opération arithmétique de champ fini GF (2^m), un système cryptographique à courbe elliptique tel qu'un système cryptographique à courbe elliptique basé sur champ primitif ou qu'un système cryptographique à courbe elliptique basé sur polynôme peut être utilisé.

Ce mode de réalisation a été décrit en tant qu'exemple concret du processus de division selon le premier mode de réalisation. Même si ce mode de réalisation est mis en œuvre en tant qu'exemple concret du processus de division selon le second mode de réalisation, des fonctions et effets similaires peuvent être obtenus.

(Quatrième mode de réalisation)

La figure 22 est une vue schématique qui représente un exemple de l'agencement d'un coprocesseur appliqué à un appareil arithmétique et à un appareil de traitement cryptographique selon le quatrième mode de réalisation de la présente invention.

Ce mode de réalisation est une modification de chacun des premier à troisième modes de réalisation et d'un appareil arithmétique conçu de façon spécifique pour des opérations arithmétiques de champ fini GF (2^m). De façon davantage spécifique, le circuit de multiplicateur basé sur les entiers 11, le sélecteur 13 et le contrôleur arithmétique d'entier 21 sont omis de l'agencement de cet appareil. Puisque le même algorithme arithmétique que celui décrit ci-avant est utilisé, un traitement de multiplication basé sur champ fini GF (2^m) est divisé selon une opération de multiplication et un modulo et le modulo est exécuté après l'opération de multiplication.

Moyennant l'agencement mentionné ci-avant, les mêmes effets que ceux des premier à troisième modes de réalisation peuvent être obtenus à l'exception de la fonction/l'effet d'une opération basée sur les entiers elle-même, de la fonction/l'effet de la commutation du mode opération basée sur les entiers et de l'opération arithmétique de champ fini GF (2^m). En d'autres termes, les mêmes effets que ceux associés aux opérations arithmétiques de champ fini GF (2^m) selon les premier à troisième modes réalisation peuvent être obtenus.

Comme il a été décrit en détail ci-avant, selon la présente invention, un appareil arithmétique et un appareil de traitement cryptographique qui permettent d'exécuter une opération arithmétique de champ fini GF (2^m) de même qu'une opération basée sur les entiers peuvent être constitués au moyen de seulement l'addition d'une architecture minimum.

En outre, sont proposés un appareil arithmétique et un appareil de traitement cryptographique qui peuvent exécuter des opérations arithmétiques sans modifier les configurations d'appareil même si le degré m d'un champ fini GF (2^m) augmente.

REVENDICATIONS

1. Procédé d'opération de produit-somme sur des nombres longs, caractérisé en ce qu'il comprend :

la réalisation d'une opération unitaire en propageant un report lors d'une opération arithmétique unitaire basée sur des entiers ; et

la réalisation d'une opération unitaire sans propager un quelconque report lors d'une opération arithmétique unitaire basée sur champ fini GF (2^m).

2. Appareil arithmétique pour réaliser une opération arithmétique de produit-somme sur des entiers longs, caractérisé en ce qu'il comprend :

un circuit arithmétique unitaire basé sur des entiers (11) ;

un circuit arithmétique unitaire basé sur champ fini GF (2^m) (12) adjacent du point de vue logique audit circuit arithmétique unitaire basé sur des entiers ; et

un sélecteur (13) configuré pour sélectionner soit ledit circuit arithmétique unitaire basé sur des entiers, soit ledit circuit arithmétique unitaire basé sur champ fini GF (2^m).

3. Appareil selon la revendication 2, caractérisé en ce qu'il comprend en outre un circuit d'additionneur (14) qui comporte un tampon pour stocker des données de résultat intermédiaire, qui additionne les données de résultat intermédiaire à des données de résultat en provenance de soit ledit circuit arithmétique unitaire basé sur des entiers, soit ledit circuit arithmétique unitaire basé sur champ fini GF (2^m) en fonction de celui qui est sélectionné par ledit sélecteur, qui propage un report lors d'une opération arithmétique unitaire basée sur des entiers et qui ne propage pas de report lors d'une opération arithmétique unitaire basé sur champ fini GF (2^m).

4. Appareil selon la revendication 3, caractérisé en ce qu'il comprend en outre un dispositif de blocage de report (16) pour stocker

un report obtenu lors d'un cycle opératoire précédent et un circuit d'additionneur des tâches de sortie (15) configuré pour additionner le report dans ledit dispositif de blocage de report à une sortie en provenance dudit circuit d'additionneur, pour émettre en sortie un bit supérieur d'un résultat d'addition en tant que report mis à jour sur ledit dispositif de blocage de report et pour émettre en sortie un bit inférieur du résultat d'addition en tant que données de résultat d'opération.

5. Appareil de traitement cryptographique caractérisé en ce qu'il réalise de façon sélective un cryptage ou un décryptage basé sur une opération basée sur des entiers au moyen dudit appareil arithmétique défini selon la revendication 2 et un cryptage ou un décryptage basé sur une opération arithmétique basée sur champ fini GF (2^m) au moyen dudit appareil arithmétique.

6. Appareil arithmétique caractérisé en ce qu'il comprend :

une unité arithmétique (4) incluant un circuit arithmétique unitaire sur des entiers (14, 15) ;

un contrôleur (5) configuré pour émettre en sortie, sur ledit circuit arithmétique unitaire sur des entiers, un signal de sélection pour sélectionner soit une opération arithmétique unitaire sur des entiers, soit une opération arithmétique unitaire basée sur champ fini GF (2^m) ; et

un contrôleur de propagation de report (33) configuré pour propager, lorsqu'une opération de produit-somme sur des nombres longs doit être exécutée, un report d'un résultat d'opération obtenu au moyen dudit circuit arithmétique unitaire basé sur des entiers suite à la réception d'un signal de sélection correspondant à une opération arithmétique unitaire basée sur des entiers et pour ne pas propager de report du résultat d'opération suite à la réception d'un signal de sélection correspondant à une opération arithmétique unitaire basée sur champ fini GF (2^m),

dans lequel une opération de multiplication basée sur des entiers et une opération de multiplication basée sur champ fini GF (2^m) sont commutées en commandant la propagation de report.

7. Appareil selon la revendication 6, caractérisé en ce que ledit circuit arithmétique unitaire sur des entiers (14, 15) comprend un additionneur complet (FA) et ledit contrôleur de propagation de report comprend un commutateur (33) sur lequel le signal de sélection et un signal de sortie de report sont entrés et réalise une commande de propagation de report dudit additionneur complet selon des unités de bits.

8. Appareil selon la revendication 6, caractérisé en ce que ledit circuit arithmétique unitaire sur des entiers (14, 15) comprend un additionneur complet et ledit contrôleur de propagation de report (33) comprend une section de sélection (33') configurée pour réaliser une commutation entre l'émission en sortie d'un résultat OU-exclusif à deux entrées obtenu par ledit additionneur complet selon des unités de bits et l'émission en sortie d'un résultat OU-exclusif basé sur le résultat et sur un report d'entrée en tant que résultat d'addition.

9. Appareil selon la revendication 6, caractérisé en ce que ledit circuit arithmétique unitaire basé sur des entiers (14, 15) additionne en propageant un report lors de l'exécution de l'opération de multiplication basée sur des entiers et additionne sans propager un quelconque report lors de l'exécution de l'opération de multiplication basée sur champ fini GF (2^m).

10. Appareil de traitement cryptographique caractérisé en ce qu'il réalise de façon sélective un cryptage ou un décryptage basé sur une opération basée sur des entiers au moyen dudit appareil arithmétique défini selon la revendication 6 et un cryptage ou un décryptage basé sur une opération arithmétique basée sur champ fini GF (2^m) au moyen dudit appareil arithmétique.

11. Appareil arithmétique caractérisé en ce qu'il comprend :

une unité arithmétique (4) incluant un circuit d'opération de produit-somme sur des nombres longs qui exécute une multiplication modulaire avec une expression de base polynôme basée sur champ fini GF (2^m) ; et

un contrôleur (5) configuré pour diviser la multiplication modulaire selon un traitement de multiplication et un modulo et pour forcer ledit circuit d'opération de produit-somme sur des nombres longs à exécuter la multiplication modulaire.

12. Appareil selon la revendication 11, caractérisé en ce que ledit circuit d'opération de produit-somme sur des nombres longs comprend un circuit de multiplicateur simple précision (12) configuré pour multiplier des données de polynôme de la base polynôme basée sur champ fini GF (2^m) sans propager un quelconque report et un circuit d'additionneur double précision (14) configuré pour additionner en utilisant un résultat de multiplication obtenu au moyen dudit circuit de multiplicateur, et ledit contrôleur commande ledit circuit de multiplicateur et ledit circuit d'additionneur lors du traitement de multiplication.

13. Appareil selon la revendication 12, caractérisé en ce que :

ledit contrôleur comprend un circuit d'acquisition de quotient (50) configuré pour établir, lors du modulo, un résultat de multiplication de deux données de polynôme en tant que données de polynôme de premier dividende, pour établir des données de polynôme modulo prédéterminées en tant que données de polynôme de diviseur, pour calculer un quotient sur la base des données de polynôme de premier dividende ou de dividende suivant et des données de polynôme de diviseur et pour acquérir des données de polynôme de quotient d'un bloc, le nombre de bits correspondant à une larguer de bus à partir d'un ordre supérieur ; et en ce que

lorsque des données de polynôme de quotient d'un bloc sont acquises lors du modulo, ledit circuit de multiplicateur et ledit circuit d'additionneur (12, 14) calculent des données de polynôme de dividende suivant en soustrayant un résultat de multiplication des données de polynôme de quotient d'un bloc et des données de polynôme de diviseur à partir de données de polynôme de dividende courant, et ledit contrôleur commande ledit circuit d'acquisition de quotient pour répéter le traitement jusqu'au calcul des données de polynôme de dividende, d'où ainsi l'obtention de données de reste.

14. Appareil selon la revendication 13, caractérisé en ce que, lors du calcul de quotient, ledit circuit d'acquisition de quotient multiplie des données d'inverse de deux blocs supérieurs des données de polynôme de diviseur et de deux blocs supérieurs des données de polynôme de dividende courant et établit un second bloc supérieur du résultat de multiplication en tant que données de polynôme de quotient d'un bloc.

15. Appareil selon la revendication 14, caractérisé en ce que ledit circuit d'acquisition de quotient calcule des données d'inverse à partir de deux blocs supérieurs des données de polynôme de diviseur et stocke les données dans une mémoire lors de l'acquisition de données de polynôme de quotient lors d'une première opération et lit des données d'inverse à partir de ladite mémoire lors de l'acquisition de données de polynôme de quotient lors d'une seconde opération et des opérations qui suivent.

16. Appareil selon la revendication 14, caractérisé en ce que, lors du calcul des données d'inverse, ledit circuit d'acquisition de quotient compte le nombre de chiffres 0 consécutifs depuis un ordre supérieur de deux blocs supérieurs des données de polynôme de diviseur, extrait des données de polynôme d'un bloc +1 bit à partir d'un ordre supérieur de telle sorte qu'un bit de poids le plus fort soit établi à 1, obtient un inverse des données de polynôme extraites, obtient des données de deux blocs en tant qu'ensemble en concaténant des données corrigées d'un bloc dont le bit de poids le plus faible est de 1 et dont les autres bits sont 0 avec un bit de poids le plus fort de l'inverse obtenu et en établissant en tant que données d'inverse un résultat obtenu en effectuant un décalage binaire des données en direction d'un coté d'ordre supérieur de la valeur de comptage du nombre de 0.

17. Appareil de traitement cryptographique caractérisé par un cryptage ou un décryptage sur la base d'une multiplication modulaire basée sur champ fini GF (2^m) au moyen dudit appareil arithmétique défini selon la revendication 11.

18. Appareil selon la revendication 11, caractérisé en ce que ledit circuit d'opération de produit-somme inclut un circuit arithmétique unitaire, fait fonctionner ledit circuit arithmétique unitaire en propageant un report lors de l'exécution d'une opération arithmétique unitaire basée sur des entiers et fait fonctionner ledit circuit arithmétique unitaire sans propager un quelconque report lors de l'exécution d'une opération arithmétique unitaire basée sur champ fini GF (2^m).

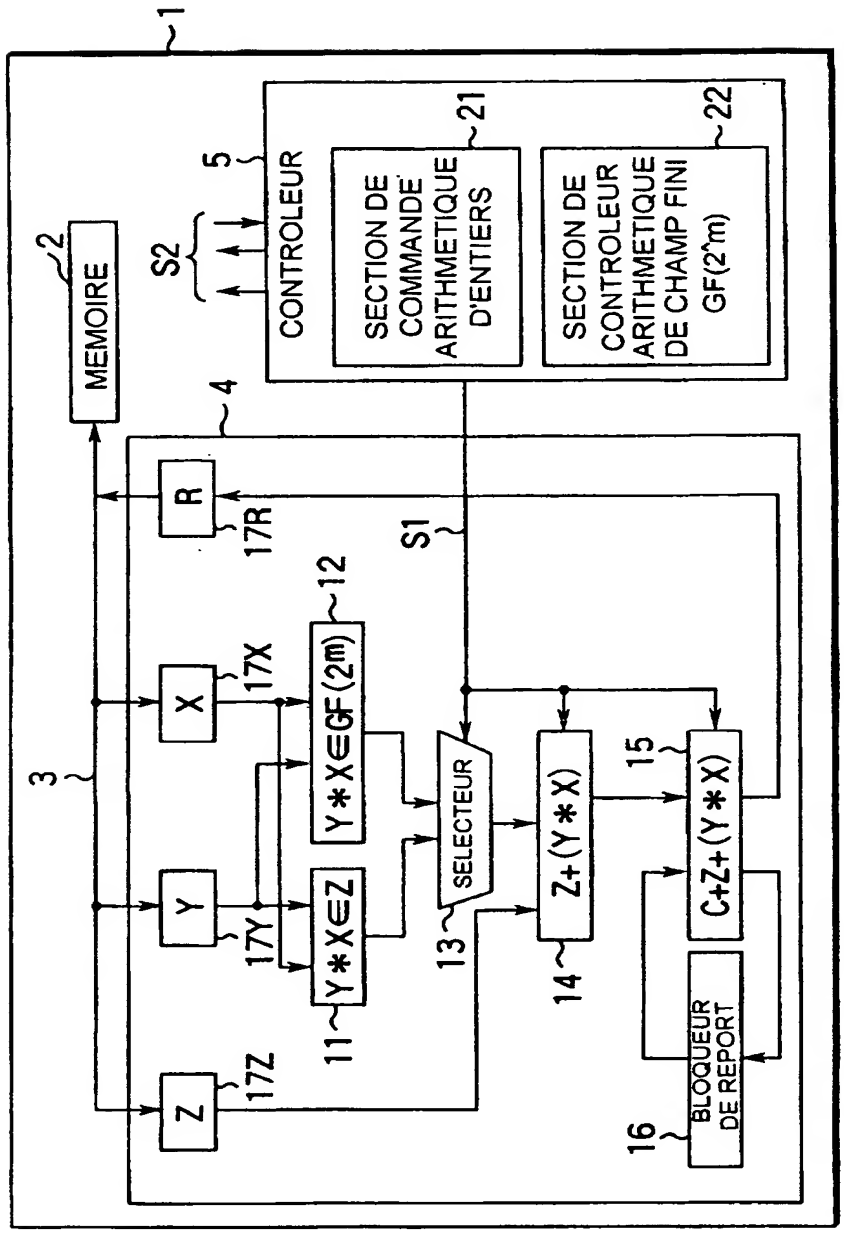


FIG.1

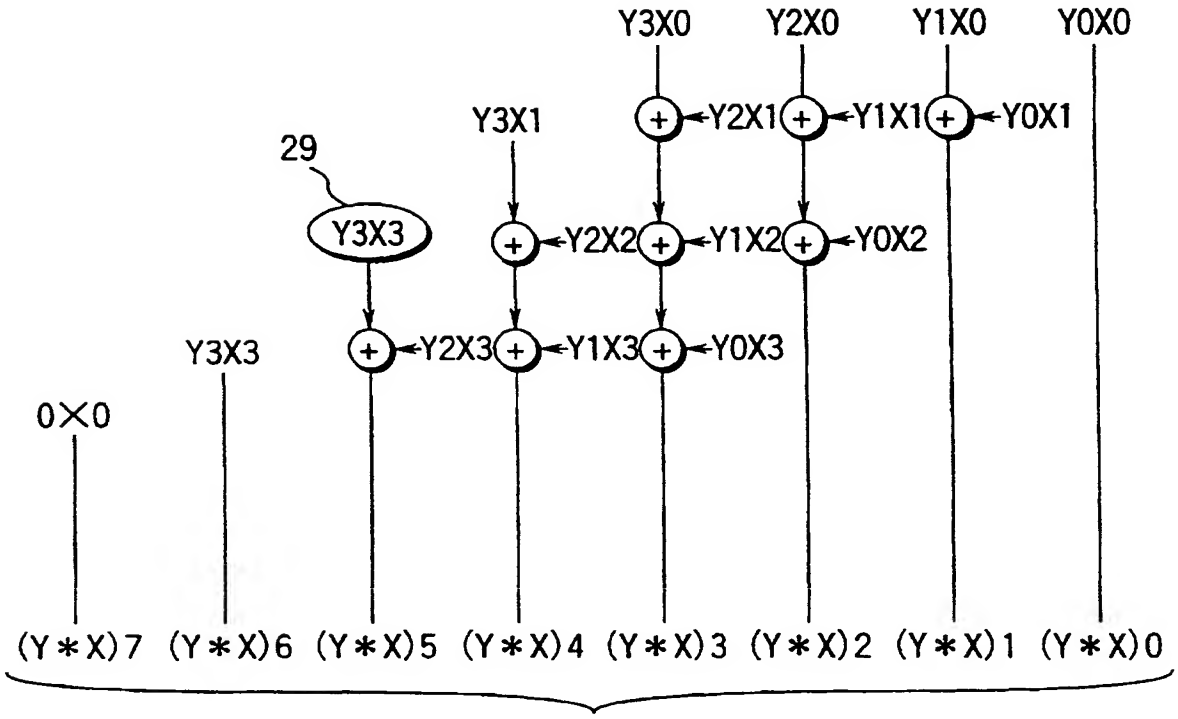


FIG.2A

FIG.2B

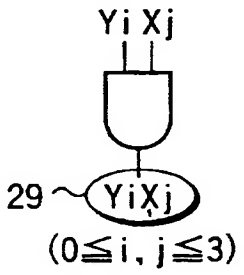
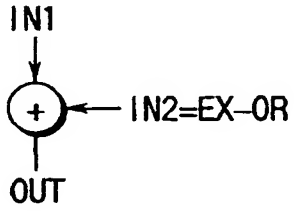


FIG.2C



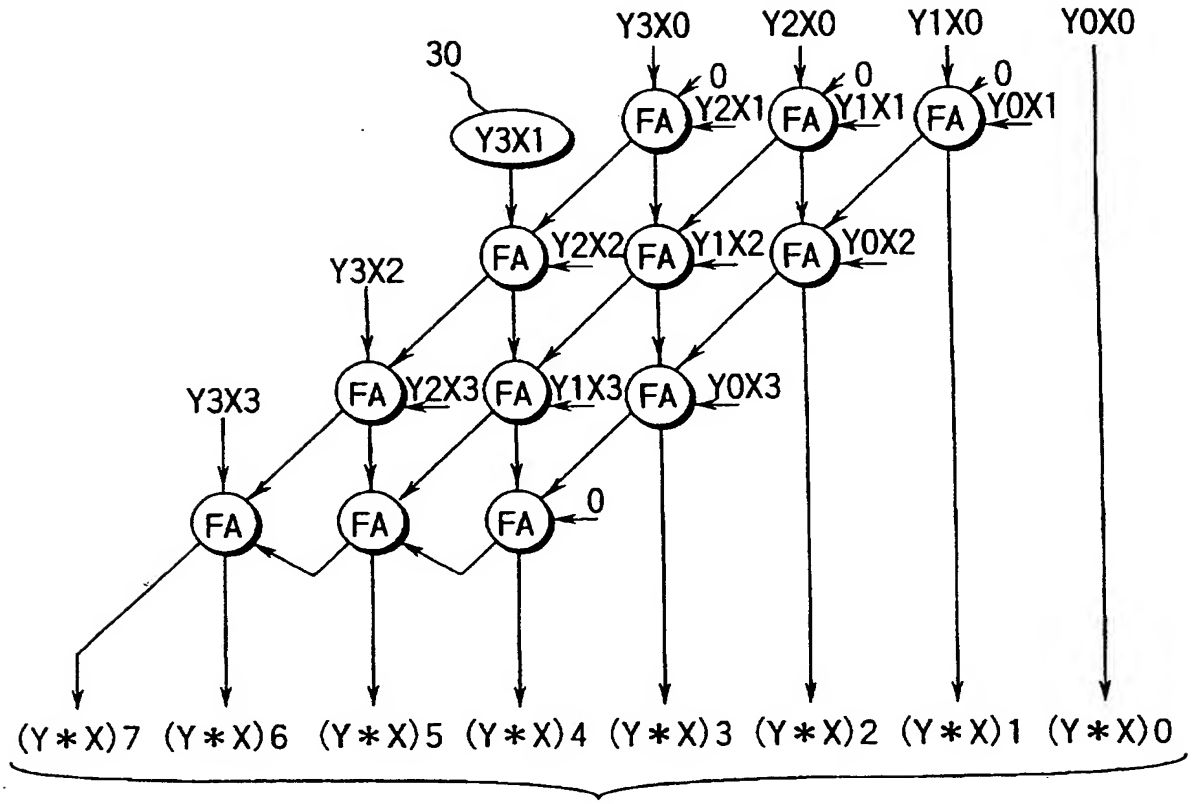


FIG.3A

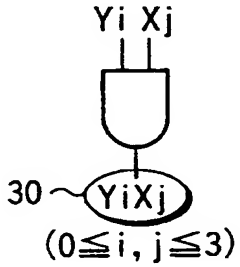


FIG.3B

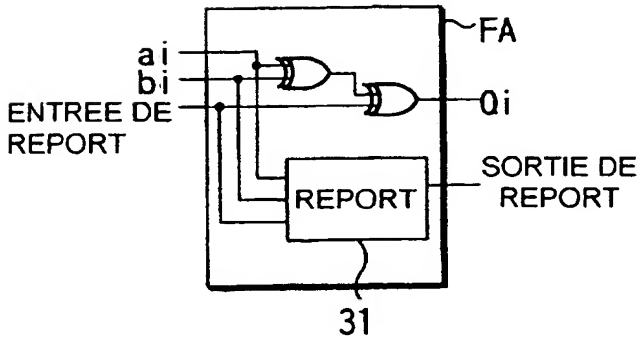


FIG.3C

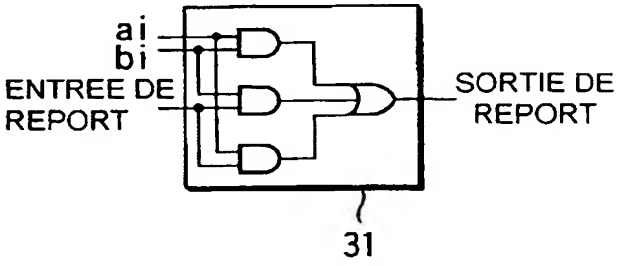


FIG.3D

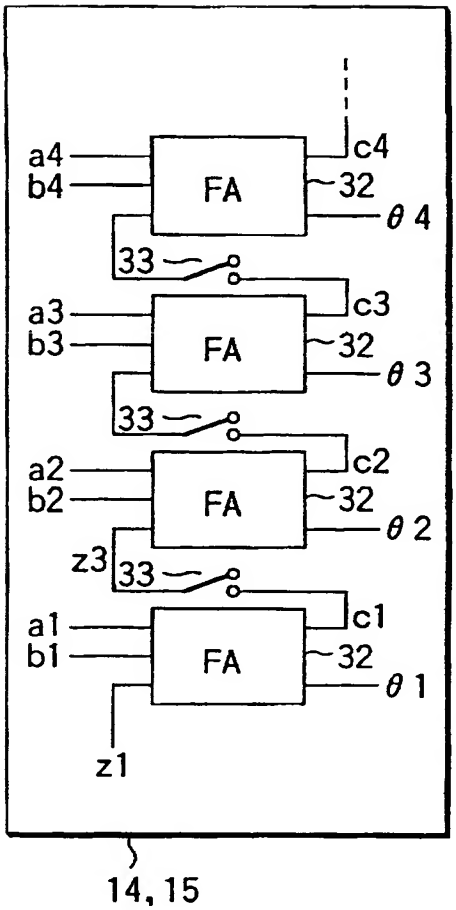


FIG.4

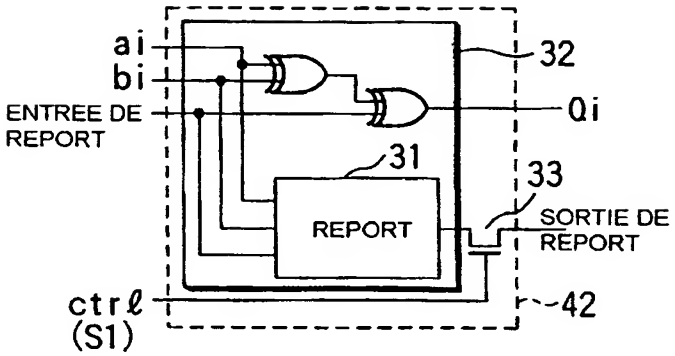


FIG.5

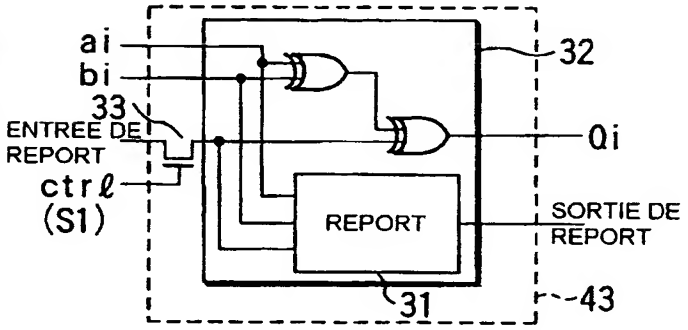


FIG.6

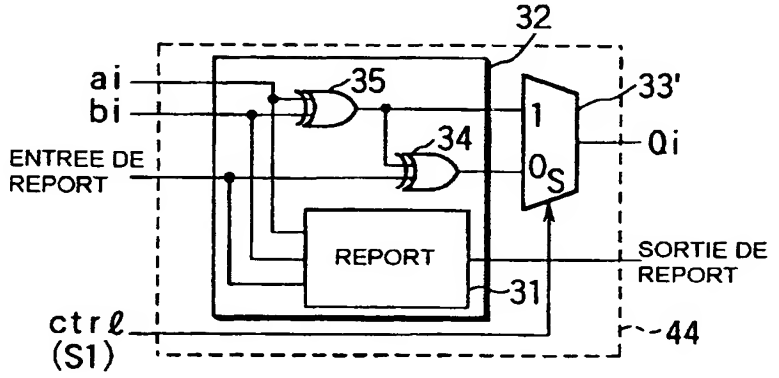


FIG.7

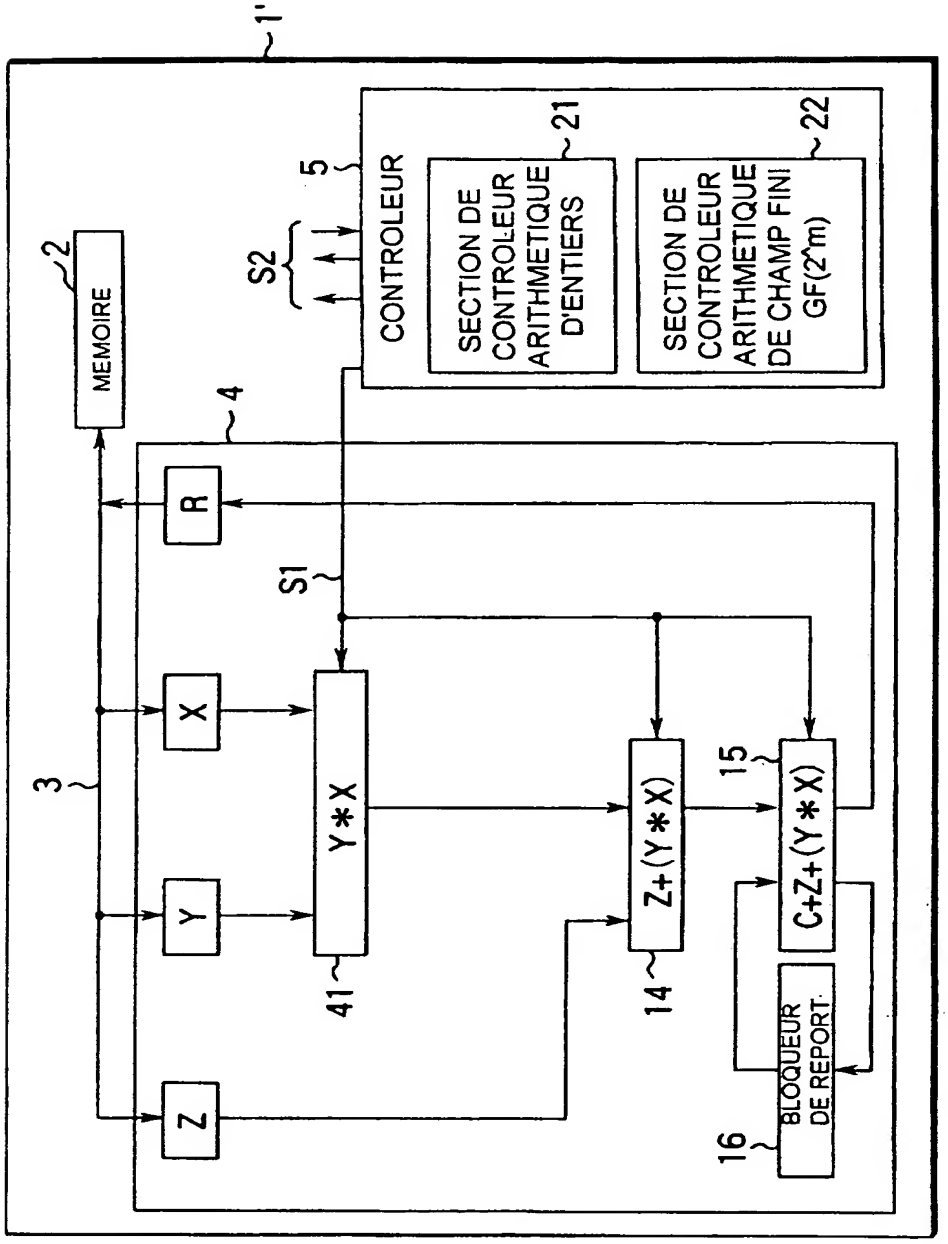


FIG.8

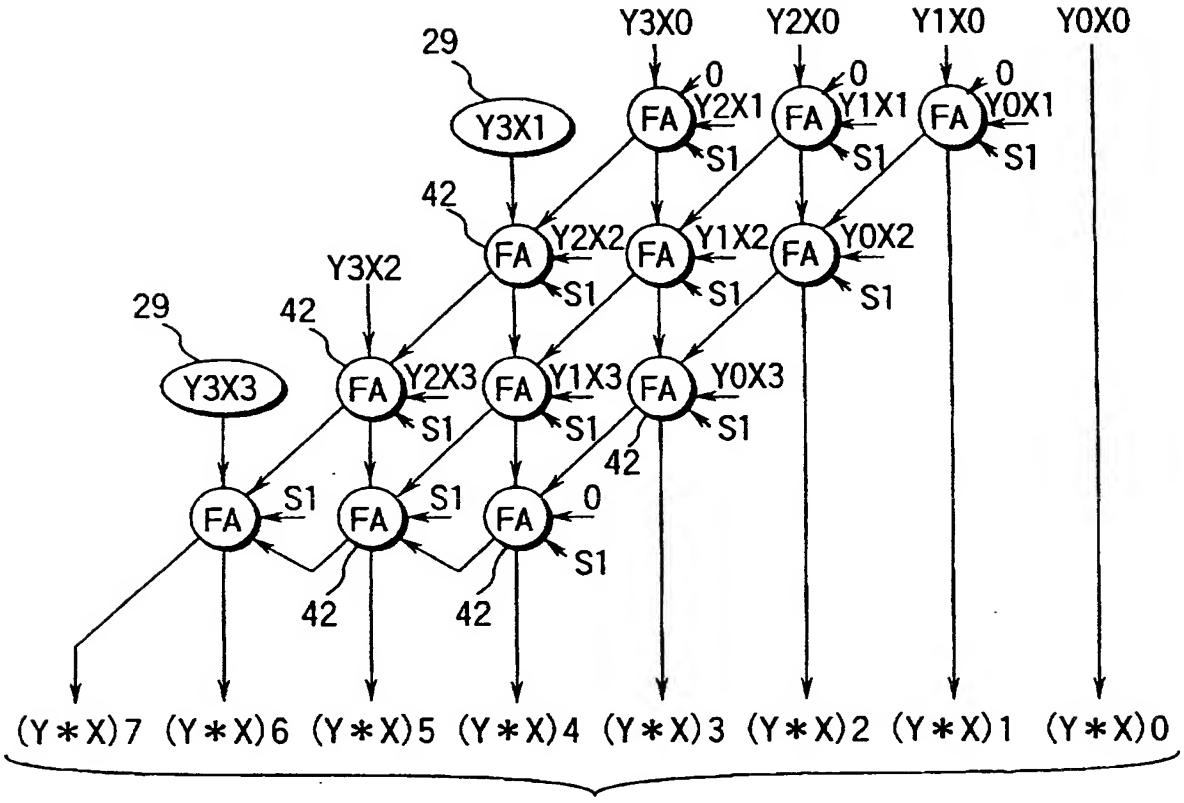


FIG.9A

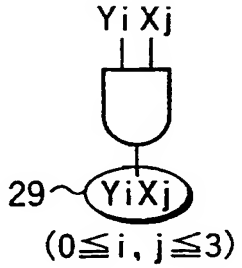


FIG.9B

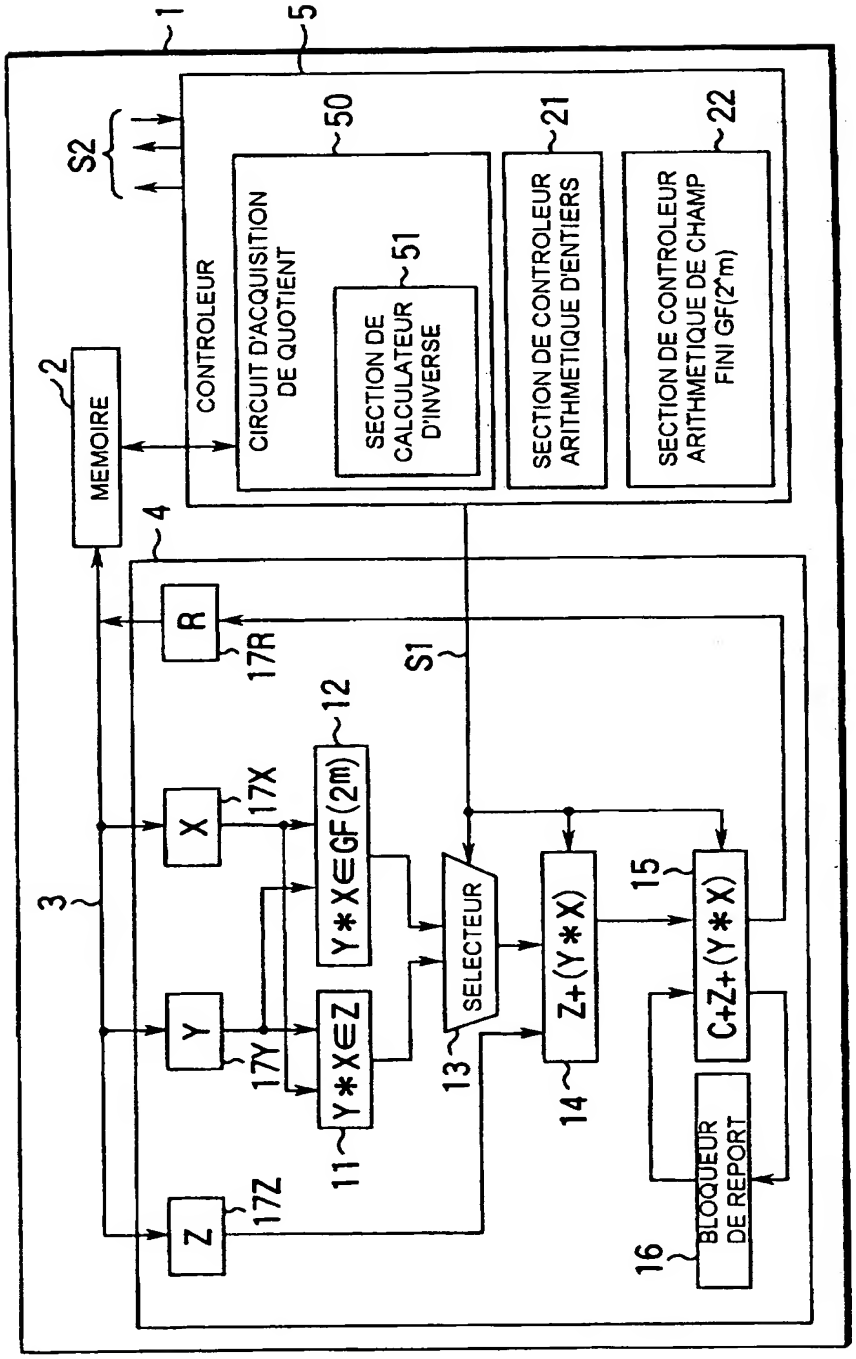

1
5
S2
50
21
22
CONTROLEUR
CIRCUIT D'ACQUISITION DE QUOTIENT
SECTION DE CALCULATEUR D'INVERSE
51
SECTION DE CONTROLEUR ARITHMETIQUE D'ENTIERS
SECTION DE CONTROLEUR ARITHMETIQUE DE CHAMP FINI GF(2^m)
2
MEMOIRE
4
R
17R
S1
12
X
17X
Y*X∈GF(2m)
3
SELECTEUR
Z+(Y*X)
15
Y
17Y
Y*X∈Z
13
C+Z+(Y*X)
14
11
Z
17Z
BLOQUEUR DE REPORT
16

FIG.10

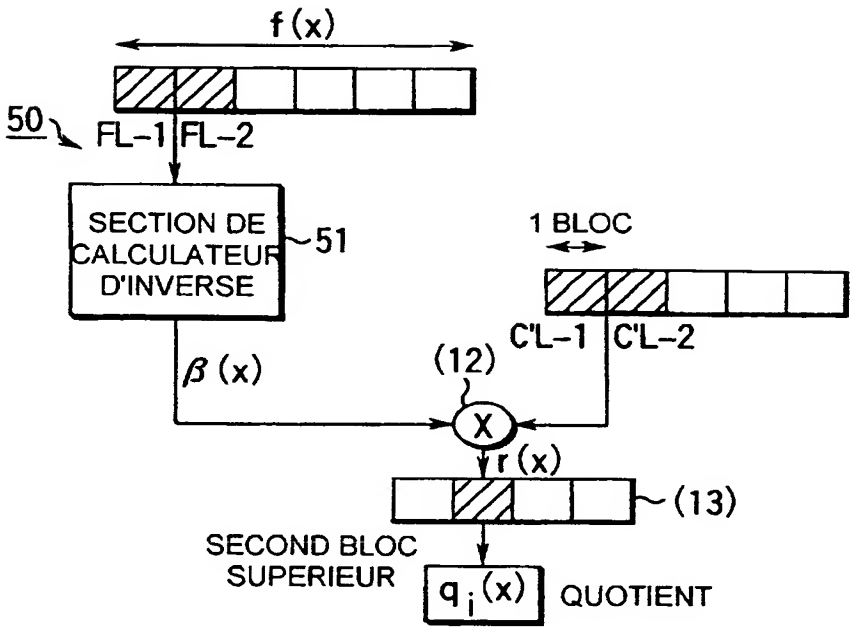


FIG.11

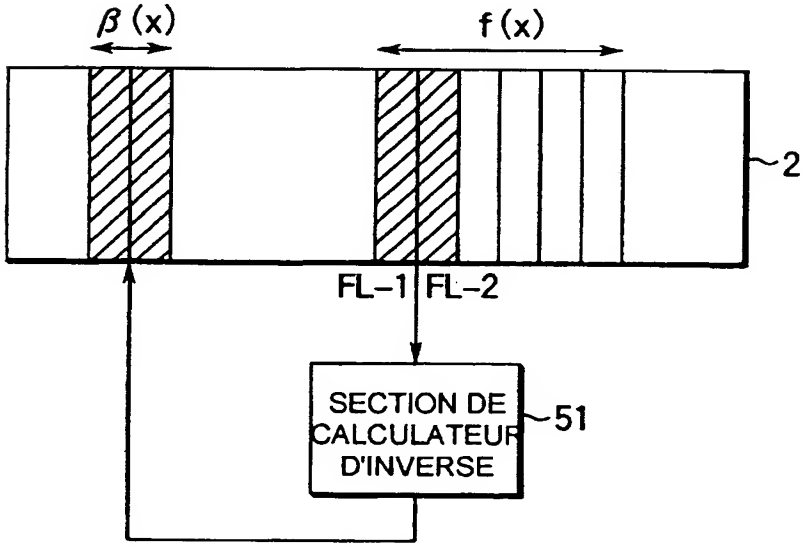


FIG.12

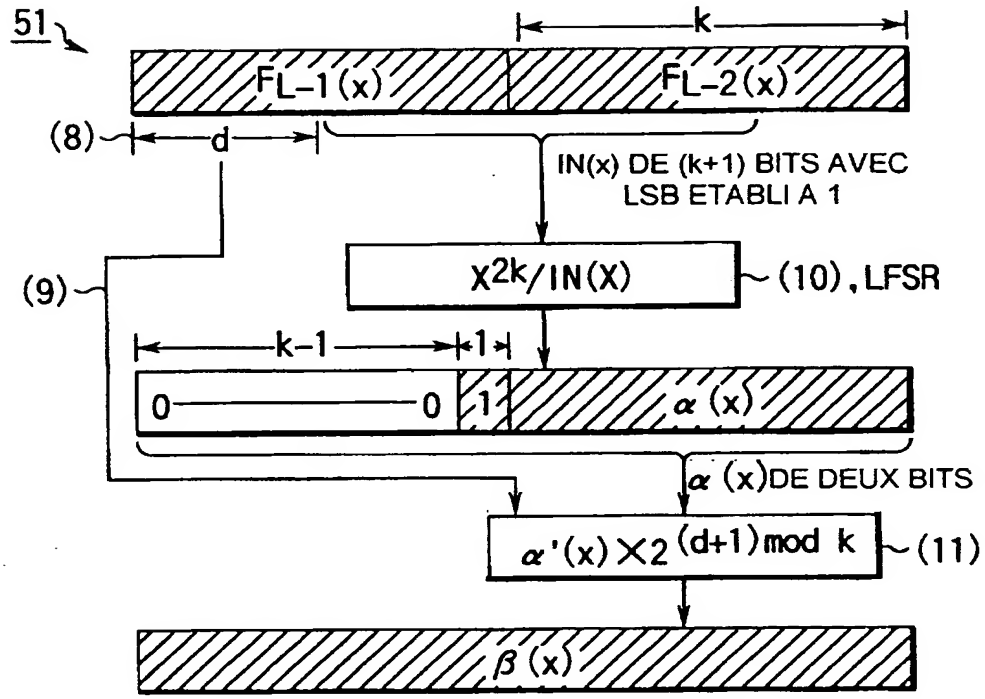


FIG.13

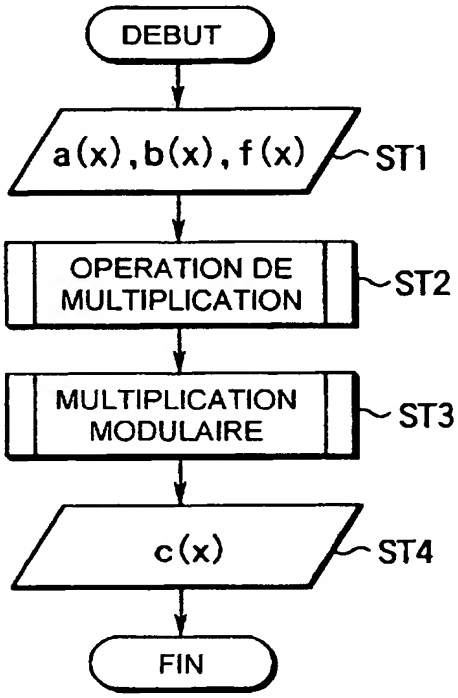


FIG.14

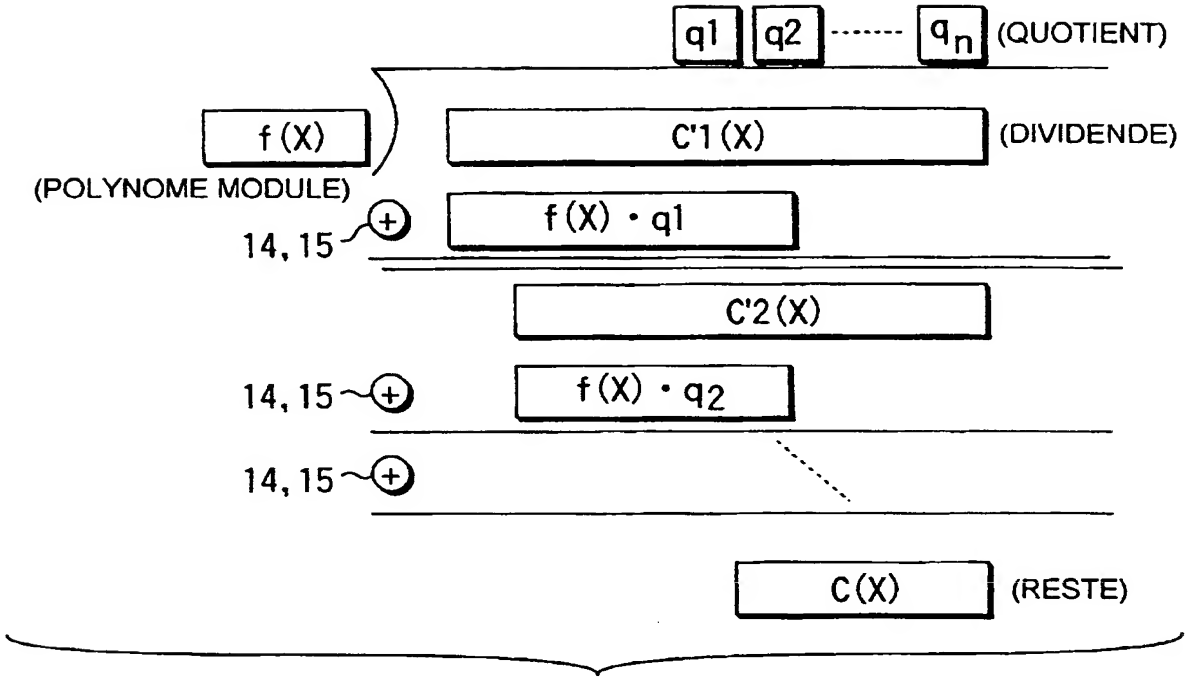


FIG.15

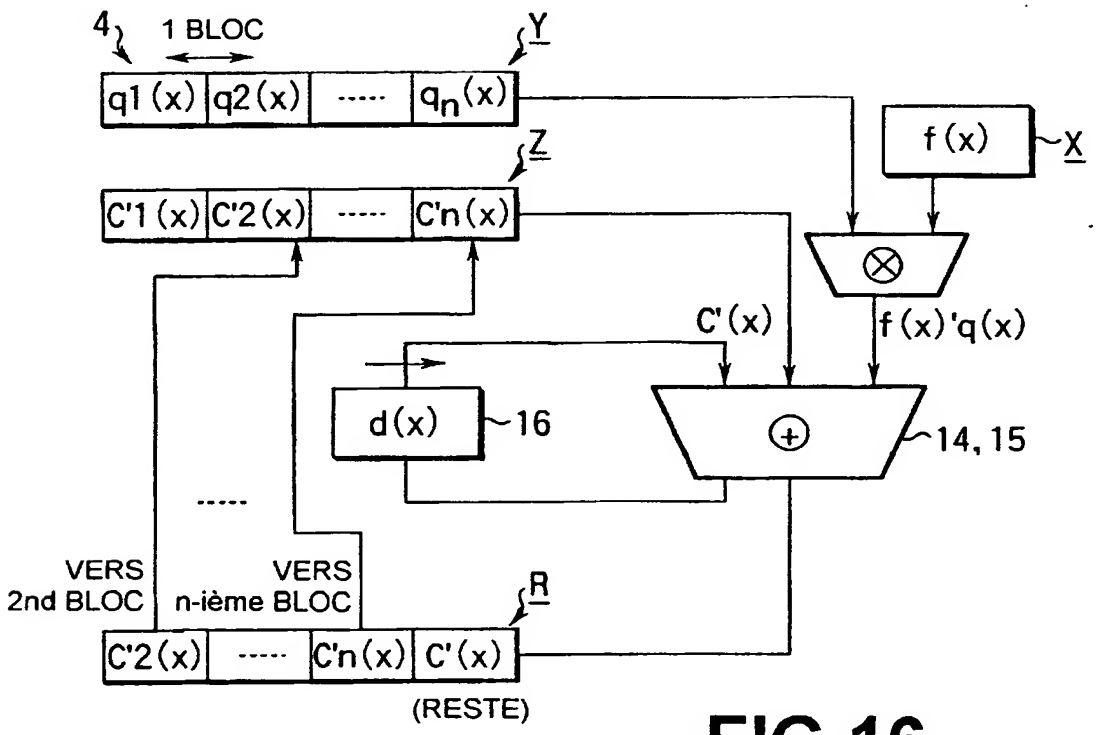


FIG.16

FIG.17

NBRE REQUIS D'HORLOGES POUR COMMANDE

COMMANDE		m=160	m=1024
ADDITION		14	68
MULTIPLICATION		64	2,116
ELEVATION AU CARRE		25	133
DIVISION	PRECALCUL	35	35
	CORPS PRINCIPAL	134	2,564

NBRE REQUIS D'HORLOGES POUR GF(2^{160})

OPERATION ARITHMETIQUE	NBRE D'HORLOGE	RAPPORT SR
ADDITION	14	ENVIRON 4,6 FOIS
MULTIPLICATION	198	ENVIRON 1,2 FOIS
ELEVATION AU CARRE	159	ENVIRON 1 FOIS

(RAPPORT SR) = (NBRE D'HORLOGES) / (NBRE D'HORLOGES DANS CCT DE REGISTRE A DECALAGE)

FIG.18

FIG.19

DIMENSION DE CIRCUIT(NBRE DE PORTES) DE COPROCESSEUR

UNITE ARITHMETIQUE	8k
CONTROLEUR	12.8k
RAM	8.5k
I/F	0.5k
TOTAL	ENVIRON 30k

FIG.20

DIMENSION DE CIRCUITS ADDITIONNELS (NBRE DE PORTES) POUR COPROCESSEUR BASE SUR ENTIERS

UNITE ARITHMETIQUE	1k
CONTROLEUR	3.8k
RAM	0 (PARTAGE)
I/F	0 (PARTAGE)
TOTAL	4.8k

DIMENSION DE CIRCUITS INDEPENDANTS
(NBRE DE PORTES DE GF(2^m)

	m=160	m=1024
UNITE ARITHMETIQUE	3.1k	3.1k
CONTROLEUR	3.8k	3.8k
RAM	2.3k	8.5k
I/F	0.5k	0.5k
TOTAL	ENVIRON 10k	ENVIRON 16k

FIG.21

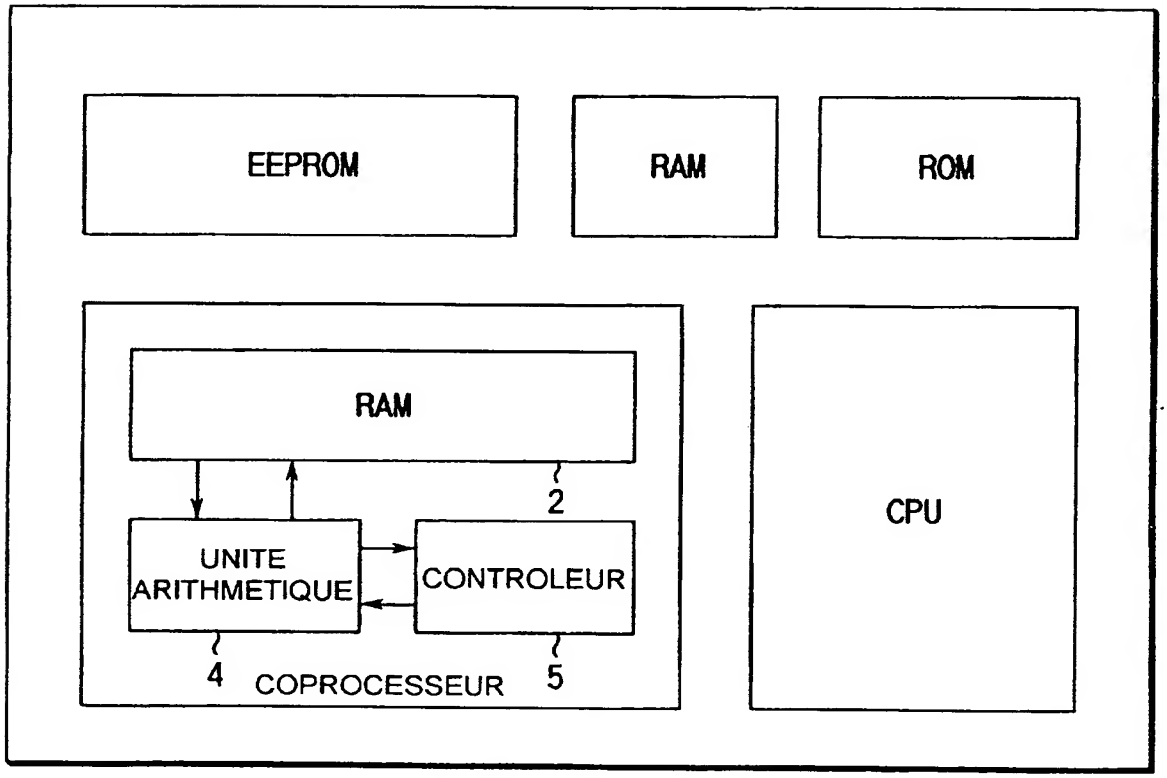


FIG.23

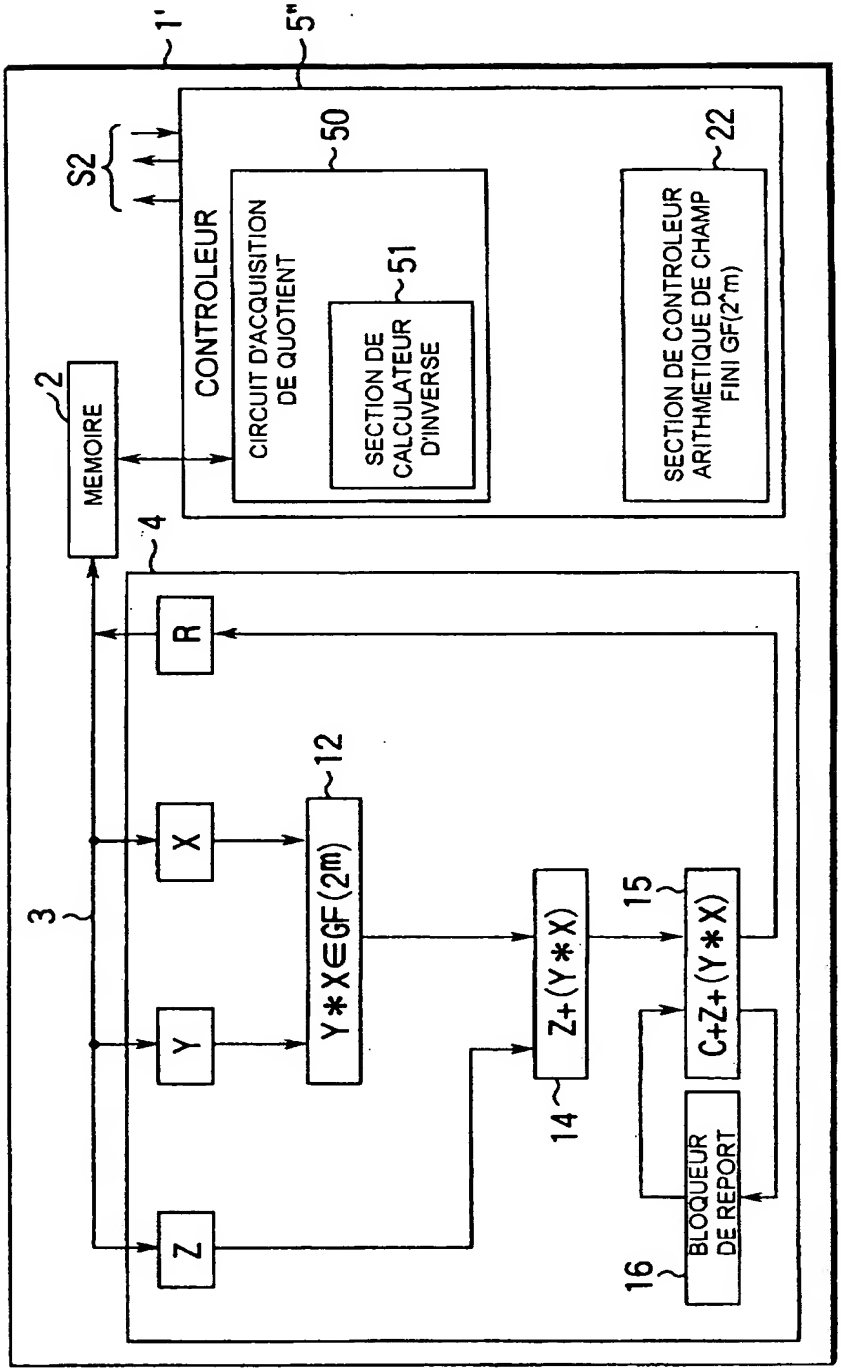


FIG.22

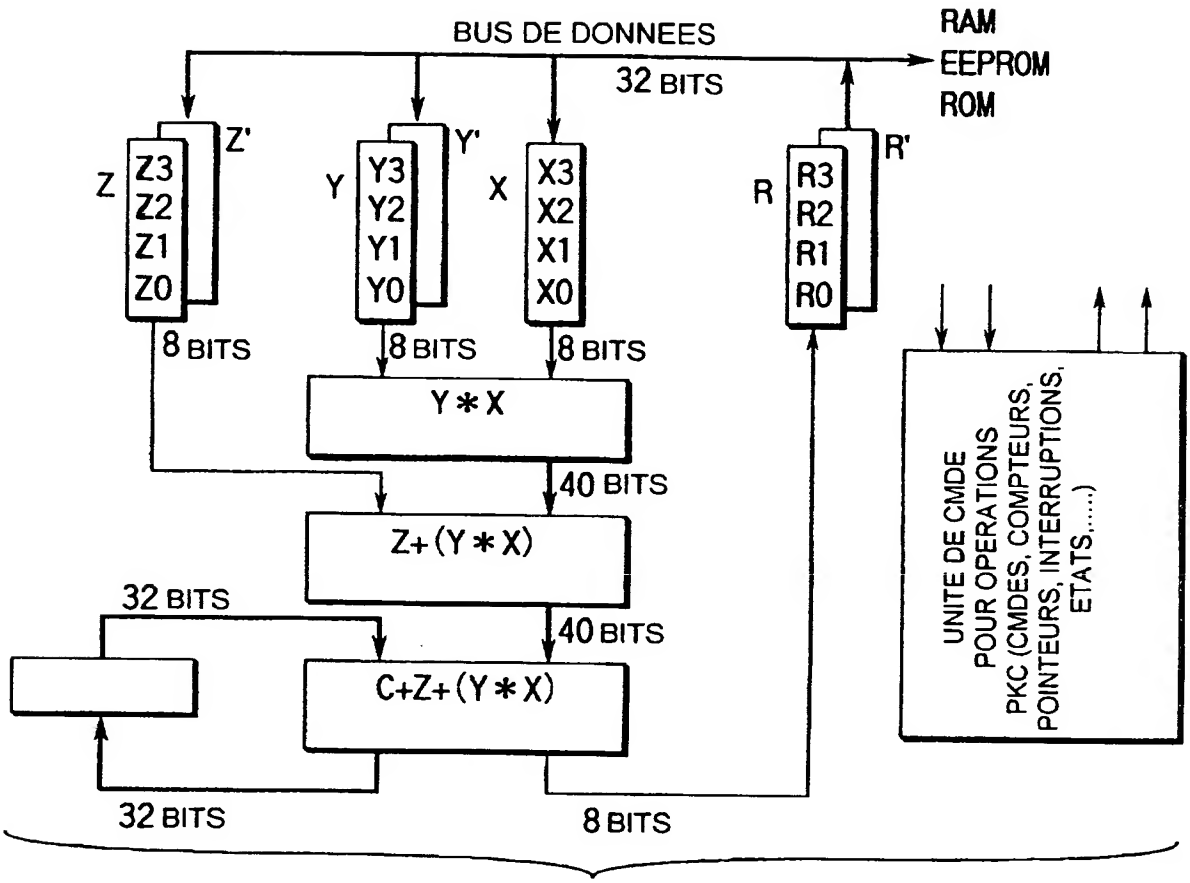


FIG.24

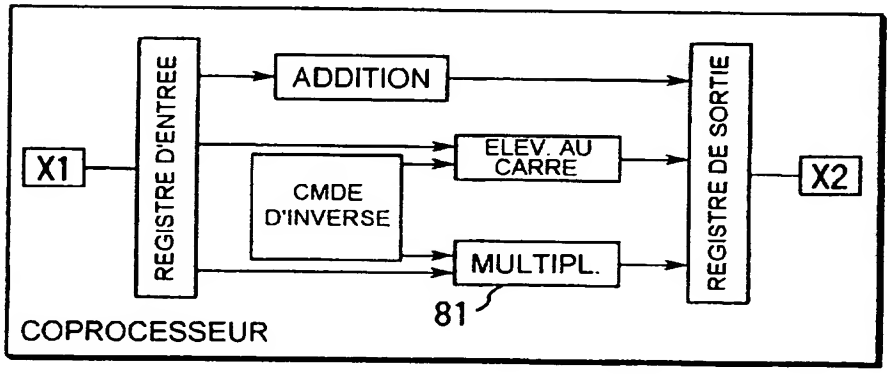


FIG.25

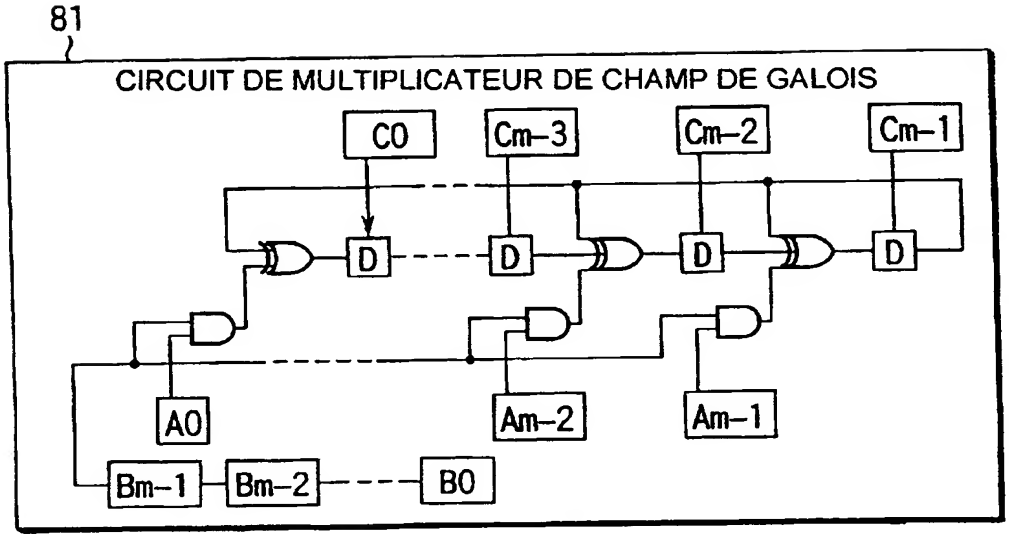


FIG.26

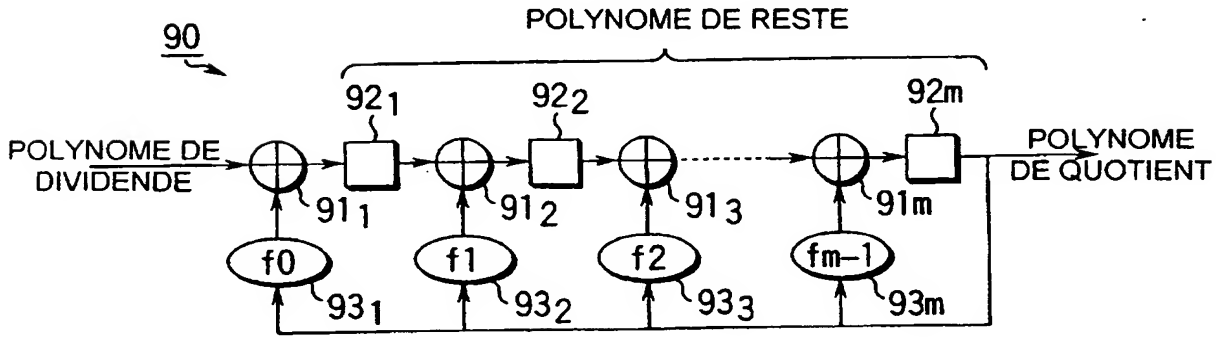


FIG.27